BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

SCHWEIZERISCHE EIDGENOSSENSCHAFT
CONFÉDÉRATION SUISSE
CONFEDERAZIONE SVIZZERA

PRIORITY DOCUMENT

SUBMITTED OR TRANSMITTED IN COMPLIANCE WITH RULE 17.1(a) OR (b)

Bescheinigung

Die beiliegenden Akten stimmen mit den ursprünglichen technischen Unterlagen des auf der nächsten Seite bezeichneten Patentgesuches für die Schweiz und Liechtenstein überein. Die Schweiz und das Fürstentum Liechtenstein bilden ein einheitliches Schutzgebiet. Der Schutz kann deshalb nur für beide Länder gemeinsam beantragt werden.

Attestation

Les documents ci-joints sont conformes aux pièces techniques originales de la demande de brevet pour la Suisse et le Liechtenstein spécifiée à la page suivante. La Suisse et la Principauté de Liechtenstein constituent un territoire unitaire de protection. La protection ne peut donc être revendiquée que pour l'ensemble des deux Etats.

Attestazione

Gli uniti documenti sono conformi agli atti tecnici originali della domanda di brevetto per la Svizzera e il Liechtenstein specificata nella pagina seguente. La Svizzera e il Principato di Liechtenstein formano un unico territorio di protezione. La protezione può dunque essere rivendicata solamente per l'insieme dei due Stati.

Bern, 29. Juni 1998

Eidgenössisches Institut für Geistiges Eigentum
Institut Fédéral de la Propriété Intellectuelle
Istituto Federale della Proprietà Intellettuale

Patentverfahren
Administration des brevets
Amministrazione die brevetti U. Kohler

Intellectual property

Patentgesuch Nr. 1997 1564/97

HINTERLEGUNGSBESCHEINIGUNG (Art. 46 Abs. 5 PatV)

Das Eidgenössische Institut für Geistiges Eigentum bescheinigt den Eingang des unten näher bezeichneten schweizerischen Patentgesuches.

Titel:
Transaktionsverfahren mit einem Mobilgerät.

Patentbewerber:
Generaldirektion PTT
Viktoriastrasse 21
3030 Bern

Vertreter:
Bovard AG Patentanwälte
Optingenstrasse 16
3000 Bern 25

Anmeldedatum: 27.06.1997

Voraussichtliche Klassen: G07G

Transaktionsverfahren mit einem Mobilgerät

Die vorliegende Erfindung betrifft ein Transaktionsverfahren mit einem Mobilgerät. Die Erfindung betrifft insbesondere, aber nicht ausschliesslich, ein Transaktionsverfahren mit einem Mobilfunktelefon, das mit einer SIM-Karte ausgerüstet ist.

Die vorliegende Erfindung wird mithilfe der als Beispiel gegebenen Beschreibung besser verständlich und durch die anliegenden Figuren veranschaulicht, welche folgendes zeigen :

Die Figur 1 ein Blockschema, das den Informationsfluss in einer ersten Ausführungsform des Systems der Erfindung zeigt, wo der Client (C) ein Mobilfunktelefon ist, vorzugsweise ein GSM-Mobilgerät, das das im Patent EP689368 beschriebene SICAP-Verfahren ausführen kann.

Die Figur 2 ein Blockschema, das den Informationsfluss in einer zweiten Ausführungsform des Systems der Erfindung zeigt, wo der Client (C) ein Mobilfunktelefon ist, vorzugsweise ein GSM-Mobilgerät, das das im Patent EP689368 beschriebene SICAP-Verfahren ausführen kann, und das POS ein Internet. oder Intranet-taugliches Gerät ist.

Die Figur 3 ein Blockschema, das den Informationsfluss in einer dritten Ausführungsform des Systems der Erfindung zeigt, wo der Client (C) ein Transponder ist, der mindestens einen Teil der SICAP-Prozeduren ausführen kann, und das POS SMS-Meldungen im GSM-Standard empfangen und/oder senden kann.

Die Figur 4 ein Blockschema, das den Informationsfluss in einer vierten Ausführungsform des Systems der Erfindung zeigt, wo der Client (C) ein Transponder ist, der mindestens einen Teil der SICAP-Prozeduren ausführen kann, und das POS ein Internet oder Intranet-taugliches Gerät ist, das SMS-Meldungen im GSM-Standard empfangen und/oder senden kann.

Die Figur 5 ein Flussdiagramm eines Zahlungstransaktionsverfahrens gemäss der Erfindung.

Die Figur 6 ein Flussdiagramm eines Nachladetransaktionsverfahrens einer SIM-Karte, gemäss der Erfindung.

Die Figur 7 ein Blockschema, das den Informationsfluss in einer fünften Ausführungsform des Systems der Erfindung zeigt.

Die Figur 8 ein Blockschema, das den Informationsfluss in einer sechsten Ausführungsform des Systems der Erfindung zeigt.

Die Figur 9 ein Blockschema, das den Informationsfluss in einer siebten Ausführungsform des Systems der Erfindung zeigt.

Das auf den Figuren 5 und 6 dargestellte Verfahren kann mit jedem beliebigen System, das auf den Figuren 1 bis 4 dargestellt ist, ausgeführt werden. Die erste und die zweite Ausführungsform benötigen beide eine spezielle SIM-Karte, die im Anhang (Fall 8) näher beschrieben wird.

Der Client (C) wird mit einem Sonderfeld IDUI (International Debit User Identification) identifiziert. Das Fixgerät wird mit einem Sonderfeld POSID (Point of Sale Identification) identifiziert. Diese beide Felder werden am Ende der Beschreibung mit einem Beispiel einer Ausführungsform erklärt.

SDR kennzeichnet eine Standardwährung. Standardwährungen im GSM-Kontext sind schon bekannt und werden, u.a., für das internationale Roaming benutzt.

Flexmart kennzeichnet ein in der Patentanmeldung PCT/CH96/00464 beschriebenes Verfahren zur Übermittlung von Aufträgen in einem Telekommunikationsnetz.

Wichtig ist zu verstehen, dass die Übermittlungen zwischen dem Client C und dem POS nicht nur Geldtransaktionen betreffen müssen. Es ist zum Beispiel auch möglich, den Client C als Schlüssel und den POS als "elektronischen Pförtner", welche das Kontrollieren des Kommens und Gehens an einer geschützten Örtlichkeit erlauben, zum Beispiel in einer Fabrik oder innerhalb der Umzäunung eines Attraktionsparkes, anzuwenden. Für diese Anwendung kann die Chipkarte mit einem abgespeicherten elektronischen

Schlüssel geladen werden. Ebenso kann mit dem erfindungsgemässen Verfahren der Zutritt zu Hotelzimmern, Theatern, Kinos, usw. verwaltet werden.

Variante 1 (Figur 1)

1. Client

Der Client (C) ist ein SICAP-taugliches GSM-Mobilgerät. Das bekannte SICAP-Verfahren, das u.a. von der Anmelderin benutzt wird, wird im Patent EP689368 beschrieben.

Der C enthält die im Fall 8 (Anhang A) beschriebene SIM-Karte, die TTP (Trusted Thyrd Party) -Funktionen ermöglicht. (GSM-SIM und kontaktlose Karte sind logisch miteinander verknüpft.). Das TTP Protokoll wird im Anhang B näher beschrieben)

2. Kasse POS X (Point-of-Sale X)

Die Kasse besitzt ein Interface mit kontaktloser Karte.

Zusätzlich hat die Kasse ein Interface entweder über GSM (SMS/Data) oder über das Fixnetz für den Belegtransfer.

3. Prozess Client / Kasse

Der Debitbetrag von der Kasse wird dem Client über die kontaktlose Schnittstelle übertragen.

Im Client wird für den Betrag ein Beleg erstellt und mit dem TTP-Prozess verschlüsselt und signiert.

Das erstellte Beleg wird der Kasse übergeben.

4. Belege-Clearing

Dem Belege-Clearing werden die Belege von z.B. eines Landes oder einer Region aller nationalen oder internationalen Clients zugeführt.

Im Clearing werden die Belege nach Operator / Finanzinstitut geordnet. Basis dazu ist die IDUI.

Die geclearten Belege werden dem Finanzinstitut zugeführt.

5. Finanzinstitut

Beim Finanzinstitut werden die Belege entschlüsselt.

Der vom Client signierte Betrag wird dem Kasse-Konto gutgeschrieben.

Das Kassa-Konto kann, muss aber nicht, beim gleichen Finanzinstitut sein.

Das Abgleichmanagement führt Kontrollbuchungen zum Konto des Mobile-Cash-Kunden durch.

Der TTP-Server führt mit dem Client die verschlüsselten Nachlade- und Checkup- Prozesse durch.

6. GSM

Mit dem GSM (oder einem ähnlichen Mobilcom-Netz) wird die mobile Flexibilität erreicht.

Der Client C ist in der Variante 1 ein Mobilgerät (MS) mit einer im Fall 8 beschriebenen erweiterten SIM-Card.

Der SICAP-TTP-Server ermöglicht die gesteuerte Kommunikation zwischen Client C und dem TTP-Server beim Finanzinstitut.

Pro GSM-Netz können eine beliebige Anzahl von Finanzinstituten bedient werden.

Variante 2 (Figur 2)

1. Client

Der Client (C) ist ein SICAP-taugliches GSM-Mobilgerät.

Der C enthält die im Fall 8 beschriebene SIM-Karte, die TTP (Trusted Thyrd Party) -Funktionen ermöglicht. (GSM-SIM und die kontaktlose Karte sind logisch miteinander verknüpft.)

2. PC Intra-/ Internet

Der Client besitzt die im Fall 8 beschriebene Funktion, die es ermöglicht, über die Tastatur des Clients und des Interfaces beim PC einen Cursor auf dem PC zu steuern und Daten zwischen Client und PC zu transferieren.

Über Inter- oder Intranet können somit auf Basis der TTP-Prozesse Dienstleistungen und Waren bestellt und bezahlt werden.

Mit der Integration von Flexmart-Funktionen (Fall 7) werden die erwähnten Prozesse auf der Ebene einzelner Produkte wesentlich vereinfacht.

Die weiteren Prozesse sind analog zur Variante 1.

Variante 3 (Figur 3)

1. Client

Der Client (C) ist im wesentlichen ein kontaktloser Chip mit SICAP-Funktionen der die TTP (Trusted Thyrd Party)-Funktionen ermöglicht. Diese Kombination kann aus einem reduzierten GSM-Chip und einem logisch verknüpften kontaklos Chip, oder einem Chip der beide Teilfunktionen erfüllt, erstellt sein.

Der Client kann in einer Uhr, als Schlüsselanhänger, usw. integriert sein.

2. Interface I

Das Interface bei dieser Variante besteht aus einem Koppler für die kontaktlose Karte, einer Tastatur und einem auf SMS-.Datenkommunikation-reduzierten GSM-MS.

Der Koppler verbindet den Client mit der GSM-Welt und der Kasse.

Die Tastatur ist das Eingabegerät für den User der den Client C benutzt

Das im Interface I integrierte, auf SMS-, Datenkommunikation-reduzierte GSM-Mobilgerät ermöglicht den verschlüsselten Nachlade-, bzw. Checkup-Prozess und den Belegetransfer.

Optional kann der verschlüsselte Nachlade-, bzw. Checkup-Prozess und der Belegetransfer über ein Modem oder ISDN-Anschluss erfolgen.

3. GSM-Welt

Innerhalb der GSM-Welt wird einerseits über SICAP der verschlüsselte Nachlade-, bzw. Checkup-Prozess und andererseits der Belegetransfer vom Client C zum TTP Server S geregelt.

Die SICAP-Plattform wird zur Drehscheibe, damit die erwähnten Prozesse für nationale sowie internationale Clients (allgemein Clients von unterschiedlichen Finanzinstituten) zu allen beteiligten Finanzinstituten (national und international) gewährleistet werden.

Die restlichen Prozesse entsprechen der Variante 1.

Variante 4 (Figur 4)

1. Client

Der Client (C) ist im wesentlichen ein kontaktloser Chip mit SICAP-Funktionen der die TTP (Trusted Thyrd Party)-Funktionen ermöglicht. Diese Kombination kann aus einem reduzierten GSM-Chip und einem logisch verknüpften kontaklos Chip, oder einem Chip der beide Teilfunktionen erfüllt, erstellt sein.

Der Client ist in einer Fernsteuerung, z.B. infrarot, integriert.

Die weiteren Funktionen sind analog Variante 3; die Kasse ist, wie bei Variante 2, ein PC.

1.1 Zahlungstransaktion

Ein Zahlungstransaktionsverfahren wird jetzt mithilfe der Figur 5 näher beschrieben. Dieses Verfahren kann auf jede beliebige Ausführungsform des Systems gemäss den Figuren 1 bis 4 angesetzt werden.

Auf dem Ablaufdiagramm 01 wird die Zahlungstransaktion dargestellt. Basiskonzept von Server, PO und Client werden in einem separaten Kapitel (inklusive Kopplung POS und Client) beschrieben. Der hier beschriebene Ablauf ist allgemein und nicht auf GSM-Prozesse beschränkt.

Schritt	Aktion
(1)	Voraussetzung ist, dass die Karte mit einem unbestimmten Betrag geladen ist.
(2)	Karte wird operativ geschaltet, z.B. mit dem Einschalten des GSM Mobilgerätes.
(3)	Der POS wird aktiviert.
(4)	Der POS ruft in einem Broadcastverfahren den nächsten, unbestimmten Client auf.
(5)	Der Client übergibt dem POS seine IDUI und die Bestätigung, dass er solvent ist. (Ob die Solvenz ausreicht, kann in diesem Moment noch nicht entschieden werden).
(6)	Der POS enthält eine Black-Liste über zu sperrende Clients (Revocation List). Der Client wird mit den Sperrlistendaten verglichen.
(7)	Vergleich stimmt, stimmt nicht.
(8)	Stimmt der Vergleich, wird ein Blockier-Flag gesetzt.
(9)	Stimmt der Vergleich NICHT, kann am POS der zu bezahlende Betrag eingegeben werden. Debit-Betrag A.
(10)	Der POS verknüpft den Debit-Betrag A inkl. Referenzwährung, z.B. SDR mit POSID und IDUI, sendet dies dem Client.
(11)	Wenn Belastungsaufforderung mit IDUI korreliert, wird Prozess weitergeleitet, wenn nicht, wird der Rückweisungsgrund am POS angezeigt.
(12)	Blockier-Flag wird geprüft.
(13)	Ist dies gesetzt, erfolgt ein Checkup mit dem Server.
(14)	Ist dies NICHT gesetzt, erfolgt der Area-Checkup.
(15)	Ist dieser NICHT gleich, erfolgt ein Checkup mit dem Server (ist wie ein Roaming-Prozess).
(16)	Check Time Out, bestimmt die Validationszeit, währenddem der Prozess ohne Check (z.B. Erneuerung des Zertifikats) ablaufen kann.
(17)	Ist der Time Out NICHT OK, erfolgt ein Checkup.
(18)	User akzeptiert Belastung mit manueller Eingabe des Passworts.
(19)	Wird die Akzeptierung verweigert oder erfolgt Time out, wird dem POS die Rückweisung mit Grundangabe signalisiert.
(20)	Ist das User-Passwort korrekt und erfolgt kein Timeout, wird der Betrag A in die Einheitswährung (z.B. SDR) umgerechnet. Damit wird ein internationaler Einsatz des Konzepts ermöglicht.
(21)	Prüft, ob der zu belastende Betrag mit dem Betrag auf der Karte gedeckt ist (Solvenz).

(22)	Ist die Solvenzprüfung negativ, wird dem POS die Rückweisung mit Grundangabe signalisiert.
(23)	Darstellung der Rückweisung mit Grundangabe beim POS.
(24)	Die neue Transaktion wird gezählt, Inkrementierung des Transaktionszähler.
(25)	Debit-Betrag, POSID und IDUI werden auf der Basis von Public Key zertifiziert (z.B. auf der Basis von ECC, Elliptic Curve Cryptosystem) und optional verschlüsselt und evt komprimiert. Es entsteht der Belastungsbeleg.
(26)	Der belastete Betrag wird auf dem Kartenkonto abgebucht.
(27)	Der Beleg wird im Kartenstack abgelegt.
(28)	Der Belastungsbeleg wird dem POS zur Abrechnung übergeben (POS-Beleg).
(29)	Der Beleg-Betrag wird am POS für den End-User ausgedruckt.
(30)	Der Beleg im POS-Stack abgelegt. Im Stack befinden sich Belege aller möglichen End-User.
(31)	Die Belege werden zum Server übertragen, oder je Zeiteinheit (Stunden, Tage) wird der POS-Stack-Inhalt übertragen (entweder Selektiv-Prozess (Einzelbeleg) oder Batch-Prozess (mehrere Belege) aus Stack).
(32)	POS-Belege werden auf Echtheit des Zertifikats überprüft (optional), dekomprimiert und entschlüsselt.
(33)	Es erfolgt ein Check über IDUI und POSID mit der Revocation List (Double Check).
(34)	Ist der Check NEGATIV, erfolgt, je nach Fall, ein Blacklist-Prozess.
(35)	Es erfolgt ein Check über Ladetoken LT, ob der vom Client gelieferte Token dem Client vom Server zugeteilt wurde (dient ebenfalls statistischen Zwecken).
(36)	Ist der Check NEGATIV, wird für den IDUI (client) ein Blacklist-Prozess gestartet.
(37)	Unterscheidung Blacklist-Prozess IDUI oder POSID
(38)	Blacklist-Prozess Client
(39)	Blacklist-Prozess POS
(40)	Ist der Check OK, wird der Beleg-Betrag dem User-Kontroll-Konto belastet.
(41)	Belegbetrag wird dem POS-Konto gutgeschrieben.
(42)	Eintrag in Liste Transaktionszähler.
(43)	Start LT/TZ Prozess, es wird überprüft, ob je Ladetoken alle Transaktionen gebucht werden.
(44)	Ist der Checkup NEGATIV, wird die Karte blockiert.
(45)	Ist der Checkup Positiv, wird die Validationszeit neu gesetzt, Timeout
(46)	Ist der Checkup Positiv, erfolgt ein Reset des Blockierflags.
(47)	Ist der Checkup Positiv, wird die neue Area gesetzt.
(48)	Karte wird blockiert.

1.2 Belastungsprozess mit unterschiedlichen Währungen

Der Belastungsprozess mit unterschiedlichen Währungen erfolgt auf der Basis der Sonderziehungsrechte oder einer andern Referenzwährung (z.B. Euro oder Dollar). Der maximale Kartenbetrag ist je nach User Class definiert. Minimal ist ein Defaultwert in SDR möglich. Jeder POS speichert den für ihn relevanten SDR-Wert (währungsspezifisch), der ihm im Einbuchungsprozess vom Server mitgeteilt wird. Je nach Kursschwankung werden die POS vom Server automatisch mit aktuellen Kursen versorgt.

1.3 Nachladeprozess

Das Nachladen der Karte mit einem Geldbetrag wird jetzt mithilfe der Figur 6 näher beschrieben. Dieses Verfahren kann auf jede beliebige Ausführungsform des Systems, gemäss den Figuren 1 bis 4, angesetzt werden.

Ein Nachladeprozess erfolgt mit dem POS und dem Client zusammen, solange dieser Prozess nicht auf GSM spezifisch angepasst ist. Je nach User-Class oder auch nach Bedarf, kann vom Server der Beleg-Stack beim Client, zwecks detaillierter Kontrolle, abgerufen werden. Nach dem Nachladeprozess kann der Stack vom Server gelöscht werden.

Schritt	Aktion
(1)	Der User schaltet seine Karte für den Nachladeprozess frei.
(2)	Der POS wird aktiviert
(3)	Der POS ruft in einem Broadcastverfahren den nächsten, unbestimmten Client auf.
(4)	Client übergibt dem POS seine IDUI und den Typ des zu startenden Prozesses. (Nachladeprozess) Generell: • Ist der Client ein GSM-Mobilgerät, sind die Teile des Prozesses „Client POS," die die Dateneingabe betreffen, auf das Mobilgerät konzentriert. • Wenn Client und POS zwei verschiedene Geräteteile sind, ist die Kommunikation zwischen den beiden Teilen gesichert, d.h. es wird ein DES TDES, RSA, ECC oder ein ähnlicher Sicherheits-prozess angewendet
(5)	Der POS enthält eine Black-Liste über zu sperrende Clients (Revocation List, dies ist ein Teil des TTP-Prozesses). Die Daten des Clients (z.B. Seriennummer) werden mit der Sperrliste verglichen.
(6)	Vergleich stimmt, stimmt nicht.
(7)	Stimmt der Vergleich, wird ein Blockierflag gesetzt
(8)	Kommunikationscheck Client POS (Signierter Prozess)
(9)	Blockierflag wird geprüft.
(10)	Ist dies gesetzt, wird die Karte gesperrt, alternativ kann ein Checkup mit dem Server, im Prozess „Zahlungstransaktion", erfolgen
(11)	Ist kein Blockierflag gesetzt, wird das Client-Password eingegeben.
(12)	Ist das Passwort OK, ist der Prozess frei für die Nachladung
(13)	Der Nachladebetrag wird eingegeben.
(14)	Wird der Betrag an einem POS eingegeben, wird POSID, IDUI und A (der zu ladende Betrag) verknüpft, wird der Betrag an einem GSM-Gerät (oder einem entsprechenden) eingegeben, ist kein POS und somit keine POSID involviert
(15)	Wenn die Daten mit IDUI korrelieren (signierter Prozess), wird der Prozess weitergeleitet, sonst Rückweisung an den POS mit Grundangabe. Der gewünschte und am POS eingegebene Nachladebetrag wird beim Client angezeigt.
(16)	Anzeige der Rückweisung des Nachladeprozess' mit Grundangabe.
(17)	Formatierung der Ladeaufforderung an den Server mit: IDUI, Debit Rest Amount (DRA) und Anzahl Zahlungstransaktionen. Optional kann

	der Server auch den Beleg-Stack auf der Karte lesen. Die Steuerung erfolgt z.B. über die User-Class und bei der Kartenausgabe oder nach Bedarf während der Nutzung bei Solvenzproblemen. Die formatierte Nachladeaufforderung wird signiert, optional komprimiert und/oder verschlüsselt. Ist der Client ein Mobilgerät ohne den POS-Eingabeteil , wird ebenfalls der POSID in die Ladeaufforderung integriert, damit der Client adressiert werden kann.
(18)	Der Server überprüft die Signatur des Nachladebelegs, optional: Dekompression, Entschlüsselung.
(19)	Tabelle von Zählern und Token der Prozesse zwischen Client und Server.
(20)	Es werden folgende Checks durchgefürt: • Beträge: Die Summe aller geladenen Beträge, inklusive der Startsumme ist gleich oder kleiner als die aller Kontrollbelastungen und des Restbetrages auf der Karte (DRA). (Die Belege zwischen Client, Clearing und Server können in diesem Moment noch nicht erfasst werden). • Ladetoken: Der Ladetoken des Client ist gleich dem des Servers(wird im Lade-, bzw. Nachladeprozess abgeglichen). • Transaktionszähler: Für jede Transaktion wird der Transaktionszähler inkrementiert TZ, in jedem Beleg wird auch TZ ebenfalls übertragen. Der beim Server, durch die vom Client zum Server transferierten Belege, inkrementierte TZ-Stand ist entweder gleich oder kleiner als der Zählerstand beim Client.
(21)	Ist der Check positiv, läuft der ordentliche Prozess, wenn nicht läuft der Rückweisungsprozess.
(22)	Ist der Check negativ, wird ein Blockierflag gesetzt
(23)	Kontostand des Users (Client) wird überprüft.
(24)	Ist der Check positiv, läuft der ordentliche Prozess, wenn nicht, läuft der Rückweisungsprozess.
(25)	Der nachzuladende Betrag wird vom Konto des Users abgehoben (inkl. Belastung allfälliger Kommissionen).
(26)	Die Rückweisung mit Prozessangabe wird aufbereitet aus den Checks Betrag, Token, Transaktion (Blockierflag) und Kontostand.
(27)	Das Nachladebeleg wird erstellt.
(28)	Signierung des Nachladebelegs.
(29)	Im Client wird die Signatur des Nachladebelegs überprüft.
(30)	Check auf Blockierflag
(31)	wenn gesetzt zu Kartenblockierung
(32)	Karte wird blockiert
(33)	Check auf Rückweisung seitens Server.
(34)	wenn Rückweisung, zu Prozessangabe
(35)	Prozessangabe gesetzt vom Server im Nachladeablauf
(36)	Wenn alle Checks im Sinne der Nachladung OK, wird das Kartenkonto mit dem geforderten Nachladebetrag gebucht
(37)	In der Karte wird der alte Ladetoken mit dem neuen ersetzt
(38)	Der Transaktionszähler auf der Karte wird zurückgesetzt
(39)	Der Timeout (Validationszeit) wird neu gesetzt
(40)	Wenn im Nachladebeleg POSID enthalten, wird neue Atea gesetzt
(41)	Neue Area wird gesetzt
(42)	Nachladebetrag wird, wenn der Prozess über das Mobilgerät läuft, am Mobilgerät angezeigt, sonst am POS.
(43)	Der Gesamtkontostand der Karte wird angezeigt.

1.4 Beleg-Clearing

Grundlage für das Beleg-Clearing sind die Belege vom POS. Grundsätzlich beinhalten die Belege alle nötigen Informationen um folgende Bedingungen abzudecken:

User von verschiedenen Ländern, Finanzinstituten.

POS in verschiedenen Ländern, Verkehrsbereichen.

Im Belegclearing werden von allen Clients (national und international) die Belege von den POS nach Finanzinstitut geordnet und diesen zugestellt.

2. Kryptographie

Für die Kryptographieprozedur werden zwei Segmente unterschieden:

2.1 Client / POS

Dieser Teil dient der Sicherstellung der Kommunikation zwischen Client und POS und basiert auf DES, TDES, RSA ECC oder einer entsprechenden Technik.

2.2 Client / Server (Finanzinstitut)

Innerhalb Client und Server (Finanzinstitut) kommt das Konzept TTP (Trusted Thyrd Party) zur Anwendung. Die nötigen Datenelemente sind auf der SICAP-Karte integriert.

Definition von IDUI und POSID

1. IDUI

International Debit User Identification

optional	gesetzt	gesetzt	optional	gesetzt	gesetzt	gesetzt
Country	Operator	User-Nr.	User-Class	Transaktions Nummer Zt	Lade Token LTs	Validation Time
			1 bis n blockiert	mmm	n	YYYY/MM/DD

2. POSID

Point of Sale Identification

optional	gesetzt	gesetzt	gesetzt	gesetzt	gesetzt	gesetzt	gesetzt
Country	Operator	Area	POS Nr	POS-Class	Datum	Zeit	Kurs
				1 bis z blockiert	YYYY/MM/DD	hh/mm	SDR oder $, Euro

In der Folge wird, mithilfe der Figur 7, eine fünfte Variante des Transaktionsverfahrens gemäss der Erfindung aufgezeigt.

Inhaltsverzeichnis

1 Einleitung

1.1 Equipment Carrier

Die folgende Anwendung stützt sich auf folgende bereits vorhandene Infrastruktur:

- GSM-Standard
- GSM-Netz
- SICAP-Plattform

1.2 Equipment Käufer

Der Käufer benötigt folgendes Zubehör:

- angemeldetes GSM-Mobiltelefon
- Vertrag mit Clearing Server

1.3 Equipment Verkäufer

Der Verkäufer benötigt folgendes Zubehör:

- EFTPOS oder ähnliches Terminal
- Vertrag mit Clearing Server

1.4 Equipment Clearingserver

Der Clearinserver benötigt folgendes Zubehör:

- Computer mit Datenbank
- „Verbindung zu Banken"

2 Funktionsweise und Ablauf

2.1 Schritt 1

Der Verkäufer tippt den zu zahlenden Betrag in die Kasse ein.
Die Kasse übermittelt an den Clearing Server die Summe sowie eine Nummer, zusammengesetzt aus der Filialennummer und der Kassenummer.

Der Kunde kreiert eine Short Message (SMS). Enthaltend den zu zahlenden Betrag und die Nummer der Filiale sowie der Kasse. Er sendet die SMS über die SMSC an den Clearing Server.

Die SMS enthält nun den Betrag, die Nummer der Filiale und der Kasse, sowie die Identifikation des Sim-Kartenbesitzers und vielleicht auch noch einen Sicherheits-PIN

2.2 Schritt 2

Der Clearing Server erhält die Daten und ergänzt sie falls notwendig.
Er weiss vom Verkäufer:

- Identität durch die Filial- und Kassennummer
- Den zu zahlenden Betrag

Er ergänzt, durch die Zugabe auf des zu verrechnenden Kontos.

Er weiss vom Käufer:

- Identität durch die Sim-Karte und PIN
- Den zu zahlenden Betrag

Er ergänzt, durch die Zugabe des zu verrechnenden Kontos

Es ist den Vetragsparteien überlassen wie die Verrechnung, vom Clearing Server aus, gehandhabt wird.

2.3 Schritt 3

Der Clearing Server vergleicht die Filial- und Kassennummer sowie den Betrag. Bei Übereinstimmung erfolgt die Transaktion.
Der Kasse wird eine Nachricht übermittelt, dass die Buchung erfolgt ist.
Der Zahlungsvorgang ist beendet.

3 Sicherheit

3.1 Identifikation

Die Kasse wird durch die Nummer der Filiale sowie der Kassennummer identifiziert. Es ist denkbar, dass weitere Identifikationsmöglichkeiten verwendet werden.
Die Übertragung erfolgt über ein gesichertes Datennetz. Wie heute bei Magnetkreditkarten.

Der Kunde Identifiziert sich auf dem Netz und somit auch beim Clearing Server durch die Sim-Karte und deren PIN.
Denkbar ist auch ein weiteren PIN auf dem Gerät oder ein persönlicher PIN beim Clearing Server, der mit der SMS mitgesendet werden müsste.
Die Datenübertragung erfolgt über das GSM Netz, was eine höchste Verschlüsselung gewährleistet (A5 A5.1).

3.2 Anonymität

Es wird nur der Endbetrag und die Einkaufsfiliale an den Clearing Server übertragen. Nicht was für Produkte gekauft wurden.
Der Kunde gibt gegenüber dem Clearing Server nur den Endbetrag und den Ort zu erkennen.
Weitere Anforderungen an den Clearing Server siehe Absatz 4.

3.3 Unstimmigkeit

Treten Unstimmigkeiten auf, z.B. der Betrag stimmt nicht überein, wird der Vorgang abgebrochen und es muss von vorne begonnen werden.

4 Clearing Server

4.1 Aufgabe des Clearing Server

Der Clearing Server übernimmt die Aufgabe der heutigen Kreditkartenfirmen.
Er nimmt die Meldungen entgegen. Identifiziert die beteiligten Parteien und deren Konten, die zur Verbuchung nötig sind.

4.2 Anforderungen an den Clearing Server

Der Clearing Server muss vertrauenswürdig und unabhängig sein und der Schweigepflicht unterliegen.

In der Folge wird, mithilfe der Figur 8, eine sechste Variante des Transaktionsverfahrens gemäss der Erfindung aufgezeigt.

Inhaltsverzeichnis

1 Einleitung

1.1 Equipment Carrier

Die folgende Anwendung stützt sich auf folgende bereits vorhandene Infrastruktur:

- GSM-Standard
- GSM-Netz
- SICAP-Plattform

1.2 Equipment Käufer

Der Käufer benötigt folgendes Zubehör:

- angemeldetes GSM-Mobiltelefon
- Vertrag mit Clearing Server

1.3 Equipment Verkäufer

Der Verkäufer benötigt folgendes Zubehör:

- Kommunikationsfähige Kasse
- Vertrag mit Clearing Server

1.4 Equipment Clearingserver

Der Clearinserver benötigt folgendes Zubehör:

- Computer mit Datenbank
- „Verbindung zu Banken"

2 Funktionsweise und Ablauf

2.1 Schritt 1

Der Verkäufer tippt den zu bezahlende Betrag in die Kasse . Zusätzlich gibt er die Natelnummer des Käufers ein.
Die Kasse kreiert eine Meldung enthaltend: Summe
Nummer enthaltend Filial- und Kassenummer
Natelnummer des Käufers

Die Meldung wird an den Clearing Server übermittelt.

2.2 Schritt 2

Der Clearing Server erhält die Daten und ergänzt sie falls notwendig.
Er weiss vom Verkäufer:

- Identität durch die Filial- und Kassennummer
- Den zu zahlenden Betrag

Er ergänzt, durch die Zugabe auf des zu verrechnenden Kontos.

Er weiss vom Käufer:

- Identität durch die Angabe der Natelnummer

Er ergänz die nötigen persönlichen Daten des Kunden.

2.3 Schritt 3

Der Clearing Server übermittelt dem Kunden eine SMS bestehend aus dem Betrag.
Der Kunde bestätigt den Einkauf mit einer weiteren SMS indem er sein OK gibt.

2.4 Schritt 4

Bei Eingang der OK-Meldung erfolgt die Transaktionsfreigabe.

3 Sicherheit

3.1 Identifikation

Die Kasse wird durch die Nummer der Filiale sowie der Kassennummer identifiziert. Es ist denkbar, dass weitere Identifikationsmöglichkeiten verwendet werden.
Die Übertragung erfolgt über ein gesichertes Datennetz. Wie heute bei Magnetkreditkarten.

Der Kunde Identifiziert sich auf dem Netz und somit auch beim Clearing Server durch dieNatelnummer. Diese wird durch die SMS überpruft und gewährleistet somit Sicherheit.
Denkbar ist auch ein weiteren PIN auf dem Gerät oder ein persönlicher PIN beim Clearing Server, der mit der SMS mitgesendet werden müsste.
Die Datenübertragung erfolgt über das GSM Netz, was eine höchste Verschlüsselung gewährleistet (A5 A5.1).

3.2 Anonymität

Es wird nur der Endbetrag und die Einkaufsfiliale an den Clearing Server übertragen. Nicht was für Produkte gekauft wurden.
Der Kunde gibt gegenüber dem Clearing Server nur den Endbetrag und den Ort zu erkennen.
Weitere Anforderungen an den Clearing Server siehe Absatz 4.

3.3 Unstimmigkeit

Treten Unstimmigkeiten auf, z.B. der Betrag stimmt nicht überein, wird der Vorgang abgebrochen und es muss von vorne begonnen werden.

In der Folge wird, mithilfe der Figur 9, eine siebte Variante des Transaktionsverfahrens gemäss der Erfindung aufgezeigt.

Inhaltsverzeichnis

1 Einleitung

1.1 Equipment Carrier

Die folgende Anwendung stützt sich auf folgende bereits vorhandene Infrastruktur:

- GSM-Standard
- GSM-Netz
- SICAP-Plattform

1.2 Equipment Käufer

Der Käufer benötigt folgendes Zubehör:

- angemeldetes GSM-Mobiltelefon
- Vertrag mit Clearing Server

1.3 Equipment Verkäufer

Der Verkäufer benötigt folgendes Zubehör:

- Normale Kasse
- Vertrag mit Clearing Server

1.4 Equipment Clearingserver

Der Clearinserver benötigt folgendes Zubehör:

- Computer mit Datenbank
- „Verbindung zu Banken"

2 Funktionsweise und Ablauf

2.1 Schritt 1

Der Kunde kreiert eine SMS bestehend aus: Nummer enthaltend Filial- und Kassennummer
Betrag

Er sind diese an den Clearing Server

2.2 Schritt 2

Der Clearing Server erhält die Daten und ergänzt sie.
Er weiss vom Verkäufer:

- Identität durch die Filial- und Kassennummer

Er ergänzt, durch die Zugabe auf des zu verrechnenden Kontos.

Er weiss vom Käufer:

- Identität durch die SIM-Karte und PIN
- den zu zahlenden Betrag

Er ergänzt, durch die Zugabe des zu verrechnenden Kontos.

2.3 Schritt 3

Der Clearing Server tätigt die Transaktion.

2.4 Schritt 4

Nach erfolgter Transaktion sendet der Clearing Server an die Verkaufstelle eine Mitteilung in Form einer SMS oder eines E-mails enthaltend:
Kassennummer
Datum; Zeit
Betrag
(Gegenkonto)

3 Sicherheit

3.1 Identifikation

Die Kasse wird durch die Nummer der Filiale sowie der Kassennummer identifiziert.

Der Kunde Identifiziert sich auf dem Netz und somit auch beim Clearing Server durch die Natelnummer. Diese wird durch die SMS überprüft und gewährleistet somit die Sicherheit.
Denkbar ist auch ein weiteren PIN auf dem Gerät oder ein persönlicher PIN beim Clearing Server, der mit der SMS mitgesendet werden müsste.
Die Datenübertragung erfolgt über das GSM Netz, was eine höchste Verschlüsselung gewährleistet (A5 A5.1).

3.2 Anonymität

Wenn auf dem Journal die Natelnummer oder das Gegenkonto angegeben ist, weiss der Clearing Server nur wo der Kunde eingekauft hat aber nicht was.
Der Verkäufer weiss nicht über seinen Gast.

4 Clearing Server

4.1 Aufgabe des Clearing Server

Der Clearing Server übernimmt die Aufgabe der heutigen Kreditkartenfirmen aber umgekehrte Reihenfolge. Clearing Server wird nicht vom Verkäufer angesprochen sondern vom Käufer. Er nimmt die Meldungen entgegen. Identifiziert die beteiligten Parteien und deren Konten, die zur Verbuchung nötig sind.

4.2 Anforderungen an den Clearing Server

Der Clearing Server muss vertrauenswürdig und unabhängig sein und der Schweigepflicht unterliegen.

Ansprüche

1. Transaktionsverfahren zwischen einem Client (C),der mit einem Mobilgerät ausgerüstet ist, und einem mit einem Telekommunikationsnetz verbundenen Point-of-sale (POS), dadurch gekennzeichnet, dass Daten aus dem Mobilgerät mit Daten aus dem POS in einem Belastungsbeleg verknüpft werden, so dass ein elektronischer Belastungsbeleg entsteht, der durch das Telekommunikationsnetz an einen mit dem Telekommunikationsnetz verbundenen Server (S) übermittelt wird.

2. Transaktionsverfahren gemäss Anspruch 1, dadurch gekennzeichnet, dass die Daten aus dem Mobilgerät eine Clientidentifizierung (IDUI, TelNr) enthalten.

3. Transaktionsverfahren gemäss Anspruch 1 oder 2, dadurch gekennzeichnet, dass die Daten aus dem POS eine POSidentifizierung (POSID, KassaNr) enthalten.

4. Transaktionsverfahren gemäss einem von den Ansprüchen 1 bis 3, dadurch gekennzeichnet, dass der Belastungsbeleg ausserdem einen Geldbetrag (A) enthält.

5. Transaktionsverfahren gemäss Anspruch 4, dadurch gekennzeichnet, dass der Geldbetrag in einer Standardwährung (SDR, Euro, Dollar) formuliert wird.

6. Transaktionsverfahren gemäss einem von den Ansprüchen 1 bis 5, dadurch gekennzeichnet, dass die Belastungsbelege verschlüsselt werden.

7. Clearing-Server, dadurch gekennzeichnet, dass er :

-elektronische Belastungsbelege von z.B. einem Land oder einer Region empfängt,

-sie nach Operator/Finanzinstitut ordnet,

-jedem Beleg dem zugeordneten Operator/Finanzinstitut übermittelt.

Unveränderliches Exemplar
Exemplaire invariable
Esemplare immutabil

Anhang A (Fall 8)

Chipkarte und Verfahren zur Kommunikation zwischen einer externen Vorrichtung und einer Chipkarte

In den Mobiltelefon-Netzen wie beispielsweise im GSM-Netz (Global System for Mobile Communication) wird die Identität der Abonnenten in einer SIM (Subscriber Identity Module)-Karte genannten Chipkarte gespeichert. Die SIM-Karte ist wegnehmbar, so dass der Benutzer die für ihn bestimmten Anrufe auf dem Mobilgerät seiner Wahl empfangen kann, indem er die SIM-Karte von einem auf ein anderes Gerät überträgt. Ausserdem sind Verfahren bekannt zum Laden der SIM-Karte mit einem Geldbetrag auf verschiedene Arten sowie zum Belasten dieses Betrages mit den Telefon-Kommunikationstaxen. Die Mobilstationen (MS, Mobile Stations), wie zum Beispiel Zellulartelefone des GSM-Typs, werden folglich aus zwei Elementen gebildet, dem mobilen Gerät und der SIM-Chipkarte.

Die SIM-Karten existieren heute in zwei genormten Formaten. Das "Full Size"-Format entspricht der Grösse einer Kreditkarte, während das "Plug-In"-Format, welches speziell an die miniaturisierten tragbaren Telefone angepasst ist, ungefähr 25 mm x 10 mm gross ist. Die Funktionalitäten der Karten mit diesen zwei Formaten sind identisch.

Die SIM-Karten enthalten im allgemeinen Datenverarbeitungsmittel, meistens einen in einem Chip integrierten Mikrokontroller. Diese

Verarbeitungsmittel enthalten einerseits eine Zone mit einem Schreib-/Lese-(Zwischen-) und/oder einem Nurlese-Speicher, welche das Abspeichern von Programmen und/oder Dateien erlaubt, insbesondere der Identifikationsdaten des die Karte besitzenden Abonnenten, sowie Berechnungs- und Verarbeitungsmittel, welche in der Lage sind, verschiedene Algorithmen auszuführen, insbesondere Algorithmen, welche die Durchführung der Abonnenten-Identifikation und der Kommunikationsverschlüsselung erlauben.

Diese Architektur der SIM-Karten, bei welcher bestimmte Aspekte im Rahmen der GSM-Norm standardisiert sind, ist sehr "offen", so dass an verschiedene Systeme von Mehrwertdiensten (VAS, Value Added Services) gedacht worden ist, welche voll von den Funktionalitäten dieser Karten Nutzen ziehen können. Insbesondere wurde an zahlreiche Dienste gedacht, welche den auf den SIM-Karten verfügbaren Speicher und/oder die Verarbeitungsmöglichkeiten des Mikrokontrollers auf der Karte zur Erweiterung der Funktionalitäten der drahtlosen Telefone verwenden.

Neue Daten oder neue Programme, welche für die Ausführung dieser neuen Mehrwertdienste notwendig sind, können im allgemeinen auf eine der drei folgenden Arten auf die Karte geladen werden :

1) Durch Einführen der Karte in eine geeignete Lese-/Schreib-Vorrichtung für Chipkarten. Die ursprünglich, d.h. bevor sie dem Kunden geliefert wird, auf die Karte geladenen Daten werden im allgemeinen auf diese Weise geladen. Dieses Verfahren kann jedoch nicht auf einfache Weise allgemein zum Aufdatieren oder Vervollständigen der auf der Karte eingetragenen Informationen nach ihrer Verteilung angewendet werden, dies aus Gründen der geringen Verbreitung der Lese-/Schreib-Vorrichtung für Chipkarten. Ausserdem muss die SIM-Karte aus der Mobilstation herausgezogen werden, um sie in eine andere Vorrichtung einzuführen, was nicht sehr praktisch ist, insbesondere für den Fall der sehr kleinen, nicht sehr praktisch zu handhabenden "Plug-In"-Karten.

2) Durch direktes Eintippen von Daten auf der Tastatur der Mobilstation. Aus Gründen der stark reduzierten Grösse der normalerweise für

die Mobiltelefone verwendeten Tastaturen sowie der beschränkten Anzahl Tasten ist diese Lösung nur für die Eingabe von sehr kurzen Daten geeignet, zum Beispiel für ein Passwort oder eine Antwort des Ja-/Nein-Typs während der Programm-Ausführung durch den Mikrokontroller der Karte, jedoch keinesfalls für die Eingabe vollständiger Programme in die SIM-Karte.

3) Die Daten und/oder Programme können auf die Mobilstation ferngeladen, zum Beispiel in Form von Kurzmeldungen (Short Messages), die einen Meldungskopf enthalten, welcher der Mobilstation ermöglicht, diese als solche zu identifizieren, und dann von der Mobilausrüstung auf die Karte übertragen werden. Diese Übertragung kann in beiden Richtungen erfolgen. Das auf den Namen der Anmelderin lautende Patentdokument EP689368 beschreibt eine Technik, welche das Fernladen von Daten und Programmen auf eine Mobilstation in transparenter Weise ermöglicht. Diese Übertragungsart kann jedoch nur von einer anderen, mit dem mobilen Funknetz verbundenen Station aus erfolgen, zum Beispiel von einem anderen Mobiltelefon aus. Die Übertragung kann ausserdem nur zum Preis der Aufnahme einer im allgemeinen gebührenpflichtigen Kommunikation im mobilen Funknetz erfolgen.

Die auf den Namen der Anmelderin lautende Patentanmeldung PCT/CH96/00464 beschreibt ein Bestellverfahren für Produkte oder Informationen mittels einer Mobilstation. Ein das Produkt und sein Lieferant unzweideutig bezeichnender Code muss in die Mobilstation eingegeben werden und wird dann zusammen mit den Identifikationsdaten des Abonnenten dem Produktlieferanten in Form von Kurzmeldungen über das mobile Funknetz übermittelt. Der Produktcode muss eine grosse Zahl von alphanumerischen Zeichen umfassen, damit das Produkt und der Produktlieferant unzweideutig bezeichnet werden. Ausserdem sind Kontrollzeichen (Parität) notwendig, um eventuelle Fehler im Produktcode zu erkennen oder zu korrigieren. Keines der obenerwähnten Mittel erweist sich als wirklich geeignet, diesen Informationstyp auf komfortable Weise in die Mobilstation einzugeben.

Umgekehrt verlangt eine bestimmte Anzahl von neuen Mehrwertdiensten, dass von einer externen Vorrichtung aus, zum Beispiel von

einem anderen Telefon aus, auf die in einer SIM-Karte gespeicherten Daten oder Programme zugegriffen werden kann.

Verschiedene Patentdokumente, insbesondere in der Gruppe H04M-001/00 der internationalen Patentklassifikation klassierte Dokumente, beschreiben Systeme, welche das Eingeben von Daten, zum Beispiel von Wahlimpulsen oder -Tönen, in einen Telefonhandapparat ermöglichen. Diese Dokumente, zum Beispiel DE2427527 oder US4130738, verlangen jedoch im allgemeinen Anpassungen des Telefonhandapparates und können deshalb nicht für den Datenaustausch mit einer konventionellen Mobilstation verwendet werden. Ausserdem erlauben diese Dokumente nur eine Einweg-Kommunikation, im allgemeinen von einer externen Vorrichtung zum Telefonhandapparat. Dies ist besonders beim Patentdokument EP0506544 der Fall. Schliesslich beziehen sich diese Dokumente im allgemeinen nicht auf die Übertragung von Daten oder Programmen in die Speicherzone einer in eine Mobilstation eingeführten SIM-Chipkarte.

Es ist folglich ein Ziel der Erfindung, eine Vorrichtung und ein Verfahren für die Kommunikation vorzuschlagen, welche für die Zweiwegübertragung von Daten und Programmen zu einer SIM-Chipkarte oder von dieser ausgehend geeignet sind.

Es ist ein weiteres Ziel der Erfindung, ein Telekommunikations-System vorzuschlagen, welches nicht die Unzulänglichkeiten der Systeme der bisherigen Technik aufweist.

Erfindungsgemäss werden diese Ziele besonders mithilfe einer Chipkarte erreicht, welche die Elemente des Kennzeichnungsteils des Patentanspruches 1 aufweist, einer Mobilstation, welche die Elemente des Kennzeichnungsteils des Patentanspruches 7 aufweist, einer Datenverarbeitungs-Vorrichtung, welche die Elemente des Kennzeichnungsteils des Patentanspruches 14 aufweist, und eines Verfahrens, welche die Elemente des Kennzeichnungsteils eines der Patentansprüche 20 oder 26 aufweist.

Insbesondere werden die Ziele der Erfindung mithilfe einer Chipkarte erreicht, zum Beispiel mit einer SIM-Karte, welche mindestens eine drahtlose Schnittstelle aufweist, die den Verarbeitungsmitteln der Karte ermöglicht, direkt mit einer ausserhalb der mobilen Kommunikationsvorrichtung befindlichen externen Vorrichtung zu kommunizieren, wobei weder die elektrischen Kontakte der Chipkarte noch die Mobilstation passiert werden.

Bei einer bevorzugten Ausführungsform der Erfindung weist die drahtlose Schnittstelle mindestens eine Spule auf und erfolgt die direkte Kommunikation zwischen der SIM-Chipkarte und einer externen Vorrichtung folglich über elektromagnetische Wellen.

So können Daten durch eine externe Vorrichtung, zum Beispiel ein anderes drahtloses Telefon oder irgendeine beliebige Datenverarbeitungs-Vorrichtung, direkt in die Chipkarte eingeschrieben oder von der Karte ausgelesen werden.

Ein Vorteil der Erfindung besteht darin, dass diese angewendet werden kann, ohne dass zwingend Änderungen an den mobilen Kommunikationsausrüstungen erforderlich sind. Die eine erfindungsgemässe drahtlose Schnittstelle aufweisende SIM-Chipkarte kann so durch einen Netzverwalter denjenigen Abonnenten verteilt werden, welche einen Mehrwertdienst abonniert haben, der dafür geeignet ist, von den Möglichkeiten dieser Karte Nutzen zu ziehen, und durch diese Abonnenten direkt verwendet werden, indem sie diese einfach in eine konventionelle Mobilstation einführen. Es ist folglich nicht notwendig, die existierenden Ausrüstungen zu ersetzen oder zu ändern, mit Ausnahme der Chipkarten, welche mit sehr geringen Kosten hergestellt werden können.

Die vorliegende Erfindung bezieht sich ebenfalls auf verschiedene Verfahren und Dienste, welche dank der Karte gemäss der vorliegenden Erfindung angewendet werden können.

Die vorliegende Erfindung wird mithilfe der als Beispiel gegebenen Beschreibung besser verständlich und durch die anliegenden Figuren veranschaulicht, welche folgendes zeigen :

Die Figur 1 eine schematische und perspektivische Ansicht einer Mobilstation, in welche eine erfindungsgemässe Chipkarte eingeführt ist, sowie einer erfindungsgemässen externen Vorrichtung.

Die Figur 2 eine schematische Ansicht einer erfindungsgemässen Chipkarte.

Obschon sich die in der Beispielsform gegebene Beschreibung insbesondere auf den Spezialfall einer zusammen mit einem tragbaren Telefon des GSM-Typs verwendeten Chipkarte des SIM-Typs (Subscriber Identity Module) bezieht, ist es wichtig, zu verstehen, dass diese ebenso mit jedem anderen Mobilstationstyp zusammen verwendet werden kann, zum Beispiel mit den Typen GSM, PCN, NMT, TACS, PDC, DCS1800 oder mit irgendeiner anderen Norm der mobilen Kommunikation, sowie mit jedem zum Speichern von Abonnentenidentitäts-Informationen in einem mobilen Kommunikationsnetz verwendeten Chipkartentyp.

Die Figur 2 veranschaulicht in schematischer Weise eine Ausführungsform einer erfindungsgemässen SIM-Chipkarte. Die Chipkarte 2, in diesem Beispiel eine Karte im Kreditkartenformat ("Full Size") weist einen konventionellen Mikrokontroller 20 auf, welcher in den Kunststoffträger 25 der Karte eingelassen und für die SIM-Funktionalitäten der Karte zuständig ist. Der Mikrokontroller 20 weist eine Schreib-/Lese- und/oder Nurlese-Speicherzone 200 sowie eine Datenverarbeitungszone 201 auf, welche in einem einzigen integrierten Schaltkreis vereinigt sind. Der Mikrokontroller 20 ist für die Anwendung der SIM-Funktionalitäten der Karte verantwortlich, wie sie zum Beispiel im Artikel "SIM CARDS" von T. Grigorova und I. Leung beschrieben werden, welcher im "Telecommunication Journal of Australia", Vol. 43, No. 2, 1993, auf den Seiten 33 bis 38 erschienen ist, sowie der neuen Funktionalitäten, welche zu einem späteren Zeitpunkt auf die SIM-Karten geladen werden. Die Chipkarte weist ebenfalls Kontaktmittel auf, zum Beispiel

einen Bereich 24 mit acht metallischen Kontakten auf der Kartenoberfläche, über welche die Karte mit der Mobilstation 1 kommuniziert, in welche sie eingeführt ist. Die elektrische Versorgung der Karte, oder mindestens des Mikrokontrollers 20, erfolgt durch die Kommunikationsstation 1 mithilfe der Kontakte 24.

Gemäss der Erfindung weist die Chipkarte 2 einen zweiten integrierten Schaltkreis 21 auf, welcher für die direkte Kommunikation mit einer externen Vorrichtung 3 zuständig ist. Der zweite integrierte Schaltkreis wird über eine Schnittstelle 22 mit dem Mikrokontroller 20 verbunden. Die Chipkarte 2 weist ausserdem eine Spule 23 auf, welche mit dem zweiten integrierten Schaltkreis 21 verbunden und in den Kunststoffträger 25 der Chipkarte eingelassen wird. Die Spule 23 kann zum Beispiel durch Wickeln eines Drahtes oder durch eine beliebige andere geeignete Technik hergestellt werden. Die Integration einer Spule in eine Chipkarte wird heutzutage gut beherrscht und wird zum Beispiel in den Patentanmeldungen WO91/16718 und WO95/33246 (beide auf den Namen Gustafson) beschrieben. Im Fall einer Chipkarte im "Full Size"-Format wird die Spule vorzugsweise zwischen zwei Kunststoffträger-Schichten 25 einlaminiert, welche die Karte bilden. Im Fall einer "Plug-In"-SIM-Karte kann die Spule entweder in den Kunststoffträger eingelassen oder mittels Klebung oder irgendeinem anderen geeigneten Mittel am Äussern dieses Trägers befestigt werden.

Die in eine Mobilstation 1 eingeführte Chipkarte 2 kann dank dieser Schnittstelle 21, 23 direkt über elektromagnetische Wellen, vorzugsweise über Funkwellen mit einer nahe bei beispielsweise etwa 120KHz liegenden Frequenz, mit einer externen Vorrichtung 3 kommunizieren, welche in symbolischer Weise dargestellt und ebenfalls mit einer Spule oder einer Antenne 30 versehen wird. Die maximale Kommunikationsdistanz ist von den Eigenschaften der Spulen 23, 30 sowie von der Sendeleistung abhängig, welche derart gewählt wird, dass eine zu starke Beanspruchung der Energiereserven der Station 1 und der Karte 2 vermieden wird; eine Reichweite von mehreren Metern ist beispielsweise ohne grössere Probleme mittels konventioneller Techniken realisierbar. Es ist wichtig, darauf zu achten, dass die Aufnahmestelle 10 für die SIM-Karte in der Station 1 um die Spule 23

herum nicht elektromagnetisch abgeschirmt ist, damit eine Funkverbindung aufgebaut werden kann.

Auf diese Weise können Daten und/oder Programme in beiden Richtungen zwischen der externen Vorrichtung 3 und der Chipkarte 2 ausgetauscht werden. Es wird so möglich, auf einfache Weise Daten oder Programme auf den Speicher 200 der Chipkarte fernzuladen, diesen Speicher von einer externen Vorrichtung 3 aus zu benutzen oder darauf zuzugreifen, oder einen beliebigen Dialog- oder Monologtyp zwischen den Verarbeitungsmitteln 20, 21 auf der Karte und einer beliebigen, für diesen Zweck geeigneten externen Vorrichtung 3 aufzubauen. Die Kommunikation zwischen der Chipkarte 2 und der externen Vorrichtung 3 erfolgt ohne Beanspruchung des mobilen Funknetzes (GSM), zu welchem die Station 1 gehört.

In diesem Beispiel wird die Chipkarte mit einem konventionellen Mikrokontroller 20, welcher Speichermittel 200 und Verarbeitungsmittel 201 aufweist, sowie mit einem Kommunikationsmodul 21 ausgerüstet, welche in der Form von zwei separaten integrierten Schaltkreisen implementiert werden. Diese Anordnung erlaubt es, Standard-Mikrokontroller 20, welche zu geringen Preisen verfügbar sind, zu verwenden und diesen ein spezifisches Kommunikationsmodul anzufügen. Der Fachmann wird jedoch feststellen, dass es ebenso möglich ist, das Kommunikationsmodul 21 im gleichen integrierten Schaltkreis wie der Mikrokontroller 20 zu integrieren, oder zum Beispiel einen Teil des Schreib-/Lese- und/oder Nurlesespeichers des Mikrokontrollers 20 in der Form eines separaten integrierten Schaltkreises zu implementieren.

Das Kommunikationsmodul 21 kann in gleicher Weise wie der Mikrokontroller 20 durch die Station 1 über Kontakte 24 gespeist werden. Bei einer bevorzugten Ausführungsform ist das Kommunikationsmodul energetisch vom Mikrokontroller 20 und von der Kommunikationsstation 1 unabhängig und wird durch die externe Vorrichtung 3 mithilfe der Spule 23 mit Energie versorgt. In diesem Fall wird vorzugsweise eine Speicherkapazität für die über die Spule 23 erhaltene Energie in der Chipkarte enthalten sein. Eine von der Station 1 oder über die Spule 23 gespiesene Pufferbatterie (Akku) kann auch auf der Karte vorhanden sein. Es ist auch möglich, zwei Spulen auf der Karte 2

anzuordnen, die eine zur eigentlichen Kommunikation mit der externen Vorrichtung 3 und die andere zur Energieversorgung des Moduls 21.

Die externe Vorrichtung 3 kann je nach der Anwendung durch einen beliebigen Apparat gebildet werden, welcher mit einer Schnittstelle 30 versehen wird, die es erlaubt, direkt über Funkwellen mit der Karte 2 zu kommunizieren, ohne Beanspruchung des mobilen GSM-Funknetzes. Im einfachsten Fall kann die externe Vorrichtung 3 aus einer weiteren erfindungsgemässen Chipkarte bestehen, welche in eine andere Mobilstation 1 eingeführt wird. Die Erfindung erlaubt so, jeden beliebigen Typ von Daten oder Programmen auszutauschen, welche auf den SIM-Karten der beiden Apparate gespeichert sind. Je nach dem SIM-Kartentyp und je nach den Verwaltungsprogrammen dieser beiden Karten ist es zum Beispiel möglich, Programme und/oder Daten von der einen zur anderen Karte zu übertragen oder zu kopieren, welche die Funktionalitäten der Karte erweitern oder Zugriff geben auf neue Dienste. Falls die Karte einen Geldbetrag enthält, von welchem die Kommunikationstaxen abgezogen werden, ist es mit einem geeigneten Kommunikationsprogramm auch möglich, den gesamten oder einen Teil des Restbetrages von der einen Karte auf die andere zu übertragen und derart eine Chipkarte mit den auf einer anderen Karte verfügbaren Beträgen aufzuladen.

Bei einer Anwendungsvariante der Erfindung wird die externe Vorrichtung 3 durch einen Rechner oder ein Terminal gebildet, welcher/s mit einer geeigneten Funkschnittstelle 30 versehen wird. Die Vorrichtung 3 wird in diesem Fall vorzugsweise mit nicht dargestellten Dateneingabe-Mitteln versehen, zum Beispiel mit einer Tastatur, und mit nicht dargestellten Datenanzeige-Mitteln versehen, zum Beispiel mit einem Display (Bildschirm). Die Vorrichtung 3 wird ausserdem vorzugsweise mit einem Kommunikationsnetz 31 verbunden, zum Beispiel über ein nicht dargestelltes Modem mit einem "Internet"- oder "Intranet"-Netz, oder mit einem beliebigen Typ eines ortsfesten oder mobilen Kommunikationsnetzes. In die Vorrichtung 3 eingegebene Daten oder Programme können dann mit Leichtigkeit über die Funkschnittstelle 30, 23 in die Chipkarte 2 kopiert werden; in umgekehrter Richtung können die in der Karte gespeicherten Daten zum Display der Vorrichtung 3 übertragen und dort angezeigt werden.

Ein interaktiver Dialog, bestehend aus einer Folge von Kommunikationen in jeder Richtung, ist ebenfalls möglich zwischen der Karte 2 und einem Rechner 3. Eine mögliche Anwendung eines solchen Dialoges betrifft die Auswahl einer Option in einem auf dem Display einer externen Vorrichtung 3 angezeigten Menu mithilfe des Mobiltelefons. Der Display der Vorrichtung 3 zeigt in diesem Fall ein Menu an, zum Beispiel eine Liste von zum Verkauf vorgeschlagenen Produkten oder von Informationen. Der Benutzer einer erfindungsgemässen Mobilstation 1 kann die Position eines Kursors in diesem Menu durch Betätigen der Kursorverschiebe-Tasten 13 auf der Tastatur seines Mobiltelefons steuern. Die Kursorverschiebe-Instruktionen werden von der Tastatur an die Chipkarte 2 übertragen und von dieser Karte mithilfe der Spule 23 zur Vorrichtung 3 gesendet. Der Benutzer betätigt eine Bestätigungstaste, zum Beispiel die Taste #, auf seiner Tastatur, um die ausgewählte Menuoption gültig zu erklären, zum Beispiel um ein Produkt zu bestellen. Der Bestätigungsbefehl wird in gleicher Weise bis zur Vorrichtung 3 übertragen, welche dann eine der ausgewählten Option entsprechende Routine ausführt. Die ausgeführte Routine kann zum Beispiel den Aufbau einer Kommunikation mit dem Lieferanten im ortsfesten oder mobilen Kommunikationsnetz 31 umfassen, mit welchem die Vorrichtung 3 verbunden ist, zum Beispiel über ein Modem, sowie die Übermittlung der Bestellung an diesen Lieferanten. In einer Variante umfasst die bei der Bestätigung einer Menuoption ausgeführte Routine die Aussendung einer Antwort durch die Schnittstelle 30 zur Chipkarte 2, zum Beispiel einen Identifikationscode des gewählten Produktes. Mindestens ein Teil der in dieser Antwort enthaltenen Daten, zum Beispiel der Identifikationscode des bestellten Produktes, werden dann in der Zone des Zwischenspeichers 200 der Chipkarte 2 gespeichert. Das auf die Chipkarte geladene Anwendungsprogramm kann dann zum Beispiel dem Produktlieferanten eine Kommunikation zusenden, zum Beispiel eine Kurzmeldung ("Short Message SMS"), welche diesen Produktidentifikations-Code enthält. Verschiedene andere Möglichkeiten von Produktbestellungen sind unter anderem in der Patentanmeldung PCT/CH96/00464.

Natürlich kann die erfindungsgemässe Chipkarte 2 auch benutzt werden um nicht nur die Position eines Objektes zu steuern, sondern auch um

mehrere Eigenschaften, wie z.B. Position, Farbe, Form, Funktion, Sichtbarkeit usw. von einem oder mehreren Objekten zu steuern.

Im Fall, wo das Menu auf dem Display der Vorrichtung 3 einer "Internet"- oder "Intranet"-Seite entspricht, welche zum Beispiel durch einen geeigneten "Browser" angezeigt wird, enthält die Kommunikation zwischen der Chipkarte und der Vorrichtung 3 vorzugsweise Instruktionen in der JAVA-Sprache (eingetragenes Warenzeichen von SUN MICROSYSTEM), welche durch den genannten "Browser" direkt interpretiert werden können. Umgekehrt ist es ebenfalls erwünscht, dass die Verarbeitungsmittel 20, 21 auf der Karte Instruktionen in der JAVA-Sprache ausführen können, damit eine gerichtete Kommunikation ermöglicht wird, welche auf Instruktionen dieses überall bekannten Programmierstandards basiert. Andere vorzugsweise objekt-orientierte Sprachen wie beispielweise Corba oder C++ k könnten auch benutzt werden.

Die externe Vorrichtung 3 kann beispielsweise auch durch eine monetäre Vorrichtung gebildet werden, zum Beispiel einen Geldmünz- oder Elektronikgeld- ("e-cash") Automaten, oder eine Registrierkasse in einem Ladengeschäft. Für den Fall, bei dem die externe Vorrichtung 3 durch einen Münzautomaten gebildet wird, kann dann die direkte Kommunikation mithilfe der Spulen 23, 30 zum Beispiel ermöglichen, den auf die Chipkarte 2 geladenen Geldbetrag vom Automaten aus nachzuladen. Der Vorteil besteht darin, dass die SIM-Karte nachgeladen werden kann, ohne dass sie aus dem Telefonhandapparat 1 herausgezogen werden muss und ohne Aufbau einer gebührenpflichtigen Funkkommunikation. Eine finanzielle Transaktion kann ebenfalls in der anderen Richtung erfolgen, durch Belastung des auf der Chipkarte 2 abgespeicherten Geldbetrages mit einem vorgegebenen Betrag und mit direkter Übermittlung des belasteten Betrages mithilfe der drahtlosen Schnittstelle gemäss der Erfindung zur externen Vorrichtung 3, zum Beispiel zu einem Automaten oder zur Registrierkasse eines Warenhauses. Eine Transaktion von Einkaufszahlungen in einem Ladengeschäft, welches mit Registrierkassen 3 ausgerüstet ist, die mit Schnittstellen 30 zum Kommunizieren mit den Chipkarten gemäss der Erfindung versehen sind, kann so die folgenden Schritte umfassen :

- direkte Übermittlung des zu bezahlenden Betrages durch die Registrierkasse 3 zur Chipkarte 2.

- Zwischenspeicherung dieses Betrages im Speicher 200 der SIM-Chipkarte.

- Ausführung einer Routine durch den Mikrokontroller 20, damit der zu bezahlende Betrag auf dem Display 12 der Mobilstation 1 angezeigt wird.

- Bei Zustimmung zur angezeigten Zahl Bestätigung dieses Betrages durch den Kunden, zum Beispiel durch Drücken auf die Taste #.

- direkte Übermittlung dieses Bestätigungsbefehls zur Vorrichtung 3 mithilfe der Schnittstelle 23-30.

Der zu bezahlende Betrag kann zum Beispiel augenblicklich dem auf der Chipkarte 2 abgespeicherten Geldbetrag belastet werden. Falls der Geldbetrag auf der Karte 2 zur Begleichung der Transaktion genügt, kann der Transaktionsbetrag der Karte belastet werden und über die Schnittstelle 23, 30 zur Vorrichtung 3 transferiert werden, nach einem beliebigen Protokolltyp und den gleichen Sicherheits- und Vertraulichkeitsregeln, wie sie sich zum Beispiel für die "e-cash"-Transfers bewährt haben.

Bei einer Variante kann der Transaktionsbetrag durch irgendein Bank- oder Finanzinstitut, bei welchem der Abonnent Kunde ist, auf ein Bankkonto des Besitzers der Vorrichtung 3 transferiert werden. Zu diesem Zweck kann im Fall der Bestätigung des auf dem Display 12 angezeigten Betrages das auf die Chipkarte 2 geladene Programm eine Instruktion zur Aussendung einer einen Belastungsbefehl enthaltenden SMS-Kurzmeldung durch die Mobilstation 1 oder durch die Vorrichtung 3 zu einem Bankinstitut enthalten.

Die externe Vorrichtung 3 kann auch durch eine Zutrittskontroll-Vorrichtung gebildet werden, zum Beispiel durch eine Vorrichtung des Typs "elektronischer Pförtner", welche das Kontrollieren des Kommens und Gehens

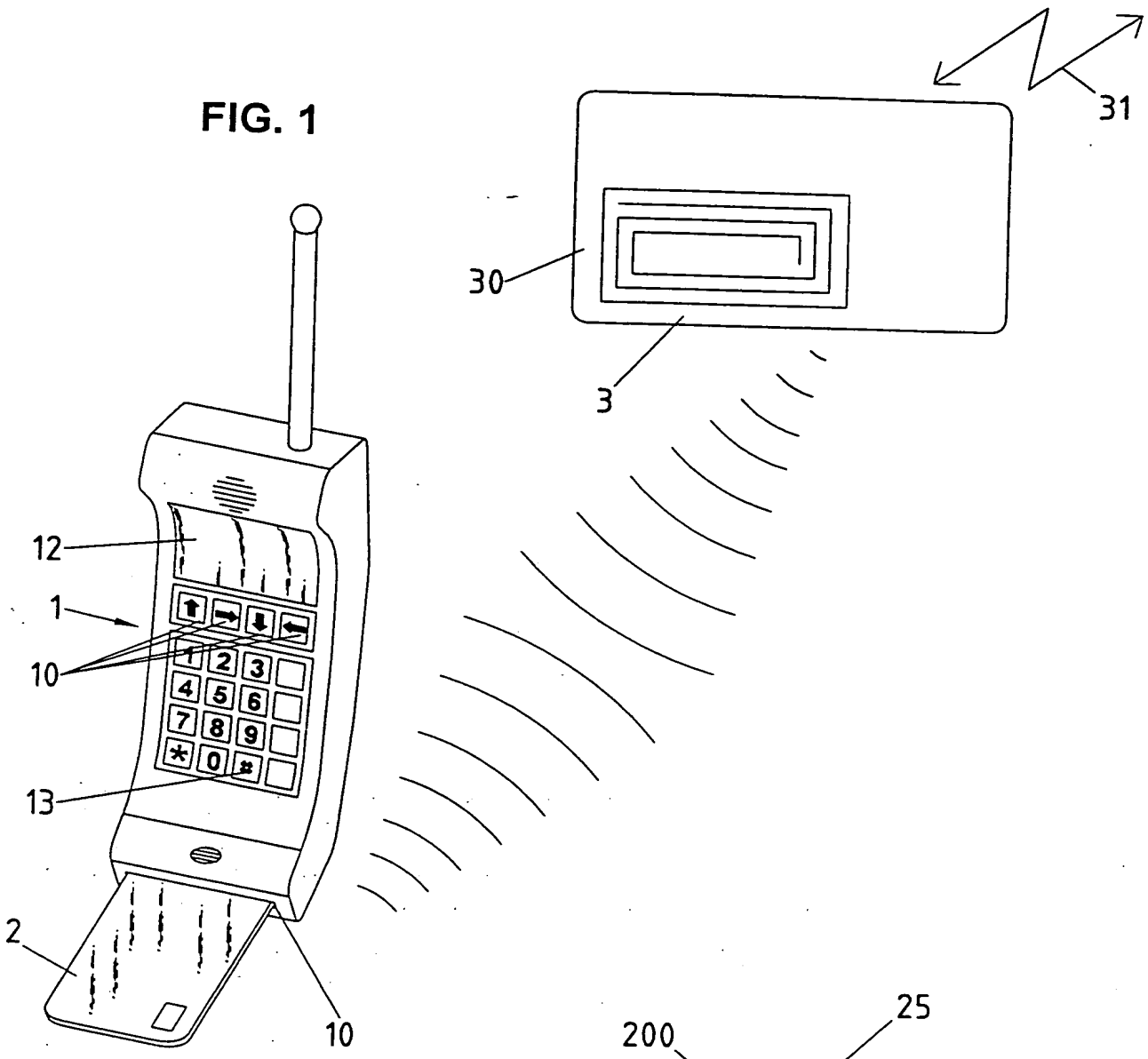
an einer geschützten Örtlichkeit erlaubt, zum Beispiel in einer Fabrik oder innerhalb der Umzäunung eines Attraktionsparkes. Für diese Anwendung kann die Chipkarte 2 mit einem im Speicher 200 abgespeicherten elektronischen Schlüssel geladen werden. Um in einer geschützten Zone der Örtlichkeit Zutritt zu erhalten, ist es also notwendig, dass eine direkte Kommunikation des beschriebenen Typs zwischen der Chipkarte 2 und der Vorrichtung 3 mithilfe der Spulen 23, 30 aufgebaut wird. Der Zutritt zur geschützten Örtlichkeit wird nur dann erlaubt, wenn es sich nach dieser Kommunikation erweist, dass der in der Karte 2 gespeicherte elektronische Schlüssel korrekt ist und seinem Besitzer das Recht zum Eindringen in die geschützte Zone gibt. Das Zutrittsverfahren kann die Aussendung umfassen von : einer Kommunikation, entweder durch die Kommunikationsstation 1 auf dem mobilen Funknetz oder durch die Zutrittskontroll-Vorrichtung 3 auf ihrem eigenen Kommunikationsnetz 31, einer Meldung des SMS-Typs, zum Beispiel für einen nicht dargestellten Zentralrechner bestimmt, welcher die Ortsveränderungen innerhalb der Örtlichkeit verwaltet und registriert. Die Verwaltung der Ortsveränderungen kann zum Beispiel die Rechnungsstellung oder die Belastung des Kontos des Abonnenten mit einem von den erfolgten Zutritten abhängigen Betrag zur Folge haben. Bei dieser Anwendung ist vorteilhaft, dass das Elektronikmodul elektrisch ausschliesslich dank der Spule 23 gespeist wird, so dass ein Zutritt sogar dann möglich wird, wenn die Batterien der Mobilstation 1 entladen sind.

Der Fachmann wird verstehen, dass diese Anwendungen lediglich in Form von nicht einschränkenden Beispielen angegeben werden. Allgemeiner ausgedrückt bezieht sich die Erfindung auf alle Verfahrenstypen, welche einen Schritt einer direkten Kommunikation mit einer SIM-Chipkarte und gegebenfalls einen Schritt einer konventionellen Kommunikation über ein konventionelles Funknetz umfassen.

Bei einer von der Erfindung abweichenden Ausführungsform erfolgt die Kommunikation zwischen den auf der Chipkarte 2 gespeicherten Daten und einer externen Vorrichtung 3 mithilfe einer Schnittstelle, welche in der mobilen Ausrüstung 1 angeordnet ist, anstatt direkt auf der Chipkarte 2. Die Kommunikation kann zum Beispiel mithilfe einer Antenne, einer Spule oder einem Infrarot-Sender-Empfänger, auf dem Gehäuse des drahtlosen Telefons 1

integriert, erfolgen. Diese Ausführungsform erfordert jedoch Abänderungen der Apparate 1 und kann folglich durch Abonnenten, welche mit konventionellen Kommunikationsstationen 1 ohne diese drahtlose Schnittstelle ausgerüstet sind, nicht auf einfache Weise angewendet werden.

FIG. 1



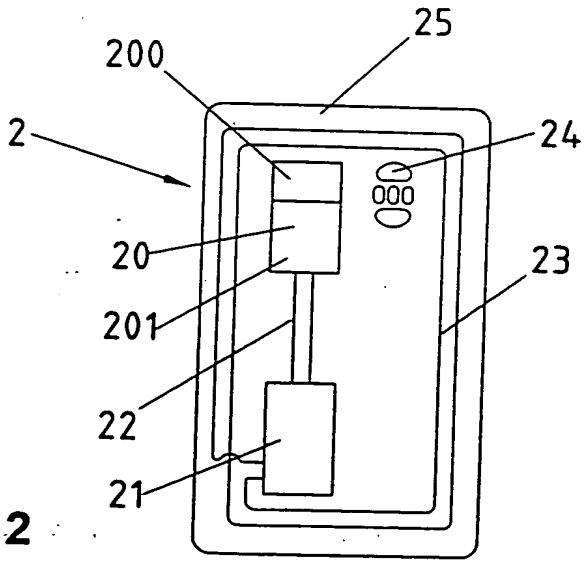


FIG. 2

Unveränderliches Ex mplar
Exemplaire invariable
Es mplare immutabile

Anhang B

TELECOM a

Forschung und Entwicklung

Peter M. Keller
Sicherheitsdienste (FE324)
Telephon: 031 / 338 10 27
Fax: 031 / 338 00 08
Email: kellerpm@vptt.ch

Grundlagen der Kryptographie und TTP's

Verschlüsselung, symmetrische und asymmetrische Algorithmen, private und öffentliche Schlüssel, digitale Signatur, Zertifizierungsinstanzen, Schlüsselzertifikate, Revocation Lists und Trusted-Third-Party Dienste

Zusammenfassung der Begriffe: (Erläuterung im Text)

Verschlüsselung / Chiffrieung	Umwandlung einer bestimmten Information (Bitsequenz) in einen unleserlichen Zustand mittels eines kryptographischen Schlüssels.
Entschlüsselung / Dechiffrierung	Zurückwandlung einer verschlüsselten Information mittels eines kryptographischen Schlüssels.
(Kryptographischer) Schlüssel	Bitsequenz, mit dessen Hilfe eine bestimmte Information ver- oder entschlüsselt wird.
Symmetrischer Algorithmus	Kryptographischer Verschlüsselungsalgorithmus, bei dem der Schlüssel für die Ver- und Entschlüsselung der gleiche ist.
Asymmetrischer Algorithmus	Kryptographischer Verschlüsselungsalgorithmus, bei dem die Schlüssel für die Verschlüsselung und Entschlüsselung verschieden sind.
Geheimer Schlüssel	Symmetrischer Schlüssel, der nur dem Absender und Empfänger einer Information bekannt ist.
Privater Schlüssel	Asymmetrischer Schlüssel, der nur einem einzigen Benützer bekannt ist und nur von diesem verwendet werden kann.
Öffentlicher Schlüssel	Asymmetrischer, zum privaten Schlüssel komplementärer Schlüssel, der allen Benützern zugänglich ist, und der veröffentlicht wird.
Schlüsselpaar	Privater und öffentlicher Schlüssel.
Digitale Signatur (Elektronische Unterschrift)	Bitsequenz als Resultat aus einer asymmetrischen Verschlüsselung mittels eines privaten Schlüssels.
Zertifizierungsinstanz / Certification Authority / CA	Unabhängige Instanz, die für die Zugehörigkeit eines öffentlichen Schlüssels zu einer bestimmten Person garantiert.
Schlüsselzertifikat / Public Key Certificate	Es bindet einen öffentlichen Schlüssel an einen Namen eines Benützers. Es enthält im wesentlichen • Eine Seriennummer, • der öffentliche Schlüssel eines Benützers • der Name des Benützers, • der Name der Zertifizierungsinstanz und • eine Gültigkeitsperiode. Dieser Information wird die digitale Signatur der Zertifizierungsinstanz hinzugefügt.

Certificate Revocation List	Von der Zertifizierungsinstanz erstellte Liste der für ungültig erklärten Zertifikate. Ein Eintrag in der Liste enthält • die Seriennummer des Zertifikats und • das Datum, an dem das Zertfikat für ungültig erklärt wurde. Die Liste wird von der Zertifizierungsinstanz digital signiert.
Querzertifikat / Cross Certificate	Zertifikat einer anderen CA.

1. Einleitung

Seit einiger Zeit lässt sich ein Trend zur Abkehr vom Dokumentenaustausch mittels Papier beobachten. Immer mehr Geschäftsinformationen fliessen heute auf elektronischem Weg von einer Abteilung zur anderen oder von einer Firma zur anderen. Fax und Email sind zwei Beispiele dafür. Bei der Übermittlung von wichtigen oder vertraulichen Dokumenten stellt sich dabei automatisch die Frage nach der Sicherheit. Leider genügen viele heute bestehenden Applikationen und Systeme den hohen Sicherheitsanforderungen, die bei der Übermittlung und Verarbeitung von heiklen Daten Voraussetzung sein sollten, nicht. Ein Internet-Email zum Beispiel kann mit ein wenig Aufwand relativ einfach abgefangen, gelesen, und verändert werden. Sogar der Name des Absenders kann ohne weiteres gefälscht werden. Dasselbe gilt für grundsätzlich für jegliche Art von Datentransfer (EDI, Fax, X.400, File Transfer, Netzwerkprotokolle, usw.), bei der ungeschützte, d.h. nicht durch kryptographische Massnahmen gesicherte Informationen übertragen werden. Nehmen wir z.B. an jemand loggt sich von zu Hause mittels eines Terminals in den Zentralrechner seiner Firma ein. Die meisten heute im Einsatz stehenden Systeme verlangen dafür einen Benützernamen und ein Passwort, das vom Benützer zu Hause in sein Terminal getippt wird und zum Zentralrechner übermittelt wird. Dieser überprüft den Benutzernamen und das Passwort und öffnet dem Benützer den Zugriff auf das System. Falls nun die Übertragung des Terminals zum Zentralrechner nicht mit kryptographischen Mechanismen geschützt ist, und das ist in der überwiegenden Mehrheit der Fälle so, dann kann theoretisch jeder, der sich auf irgendeine Weise Zutritt zu der Telephonleitung des Benützers verschaffen kann, die ganze Session z.B. auf Tonband aufnehmen. Dieses kann er anschliessend in Ruhe analysieren und den Benützernamen und das Passwort herausfinden. Nun kann er sich selber in das System einloggen, da er nun alles hat, was er dazu braucht, nämlich den Benützernamen und das Passwort. Dieses Beispiel veranschaulicht die Problematik, die entsteht, wenn Passwörter oder allgemein schützenswerte Daten offen übermittelt werden. Dabei spielt es keine Rolle, über welche Kanäle die Übermittlung stattfindet. Die Situation ist die selbe für eine Telephonleitung, ein LAN, ein Mobiltelephon oder eine Satellitenverbindung.
Ein gutes Beispiel für diese Problematik ist das Internet. Die Basis jeder Kommunikation über das Internet ist TCP/IP – eine Serie von Kommunikationsprotokollen, die heute aber auch für Netze, die nicht am Internet angeschlossen sind, eingesetzt werden. TCP/IP ist heute sogar das am meisten verwendete Transportprotokoll. Das Basisprotokoll der TCP/IP Serie ist das Internet Protokoll (IP). Nun haben die Erfinder von IP es seinerzeit unterlassen, Sicherheitsmechanismen in das Protokoll einzubauen. Die Grundeinheit des IP-Protokolls, das IP-Packet, kann somit unbemerkt durch jeden, der auf dessen Reise Zugriff darauf hat, abgeändert werden. So enthält das IP-Packet z.B. die Absender- und Empfängeradresse des Packetes, die die beliebig ausgewechselt und verfälscht werden können. Das gleiche Problem bietet sich für die anderen Protokolle der TCP/IP Serie.
Es gibt darum diverse (neue) Protokolle, die zwar alle auf TCP/IP aufbauen können, deren Sicherheit jedoch in der Applikationsebene selber implementiert ist.

Solche neue Protokolle oder Dateiformate sind z.B.:

- PEM (Privacy Enhanced Mail): Internet Standard für sicheres Email
- X.400 (ITU/ISO-Standard für Email): Enthält Sicherheitsfunktionen ab Version 1988
- SET (Secure Electronic Transactions): Industriestandard für Online Kreditkartentransaktionen (VISA, Mastercard, IBM, Netscape, Microsoft, etc.).
- S-HTTP: (Secure Hypertext Transport Protocol): Sicheres WWW-Grundprotokoll.
- SSL (Secure Socket Layer): Sicheres Kommunikationsprotokoll, basierend auf TCP/IP. Industriestandard. Wird heute u.a. im Netscape Navigator und im Microsoft Explorer (die am meisten gebrauchten WWW-Browser) eingesetzt.
- IPv6 (Internet Protokoll Version 6): Neue Version des Basisprotokolls der TCP/IP Serie. Enthält neu Sicherheitsfunktionen.

Alle diese sicheren Protokolle und Formate bauen auf sog. Public Key Systemen auf. Wie diese im Detail funktionieren, soll im folgenden dargelegt werden.

2. Sicherheitsanforderungen

Beim Austausch von Daten unterscheidet man zwischen folgenden Anforderungen an die Sicherheit:

- **Vertraulichkeit:** Sicherstellung, dass eine Information nicht für Unbefugte zugänglich oder lesbar gemacht wird.
- **Authentifikation:** Prozess, in dem die Authentizität überprüft wird.
- **Authentizität:** Beweis einer Identität. Sie bewirkt die Gewissheit, dass eine Person, eine Maschine oder ein Prozess tatsächlich derjenige ist, für den er sich ausgibt.
- **Authentizität einer Information:** Gewissheit, dass der Absender/Hersteller einer Information (Person, Maschine, Prozess) authentisch ist.
- **Nichtabstreitbarkeit des Ursprungs / Herkunftsbeweis:** Der Absender einer Information kann *nicht abstreiten*, dass die Information von ihm stammt.
- **Integrität:** Sicherstellung der Konsistenz der Information, d.h. Schutz vor Veränderung, Hinzufügung oder Löschung von Informationen.

Nachfolgend wird hier statt des Begriffs "Information" der Begriff "Meldung" verwendet. Eine Meldung ist eine Information[1], die von einem Absender an einen Empfänger übermittelt wird. Die Begriffe "Absender" und "Empfänger" sind hier sehr weit gefasst. Als Absender oder Empfänger können Personen, Maschinen, einzelne Hardwaremodule oder sogar einzelne Prozesse gemeint sein.

Die Authentizität des Absenders, Integrität der Information und Nichtabstreitbarkeit des Ursprungs der Information werden durch die Verwendung einer sog. **digitalen Signatur** erreicht. Eine Digitale Signatur ist ein kryptographischer Code (d.h. eine Bitsequenz), der für eine bestimmte Information einzigartig ist, und für dessen Herstellung ein kryptologischer Schlüssel (ebenfalls eine Bitsequenz), den nur der Verfasser besitzt, benötigt wird. Die Digitale Signatur kann demnach nur vom Besitzer des privaten Schlüssels hergestellt werden kann. Sie wird normalerweise der Originalmeldung beigefügt.

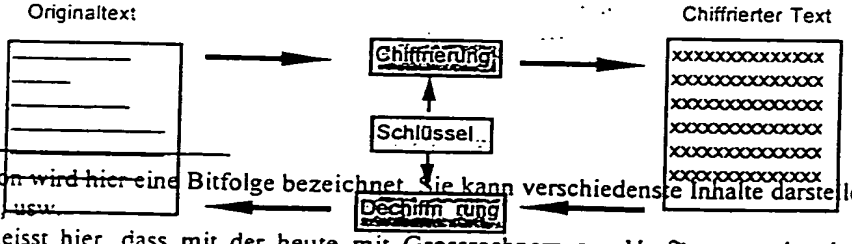
Die Vertraulichkeit der Informationsübertragung wird durch **Verschlüsselung** erreicht. Sie besteht darin, dass die Meldung mit Hilfe eines Verschlüsselungsalgorithmus und einem kryptographischen Schlüssel (Bitsequenz) in einen unleserlichen Zustand verwandelt wird. Aus der auf diese Art verwandelten Meldung kann die Ursprungsinformation nicht zurückgewonnen werden, es sei denn man kenne den zum Entschlüsseln notwendigen Schlüssel.

Wie das im Detail funktioniert, wird im folgenden dargelegt.

3. Symmetrische und asymmetrische Verschlüsselung

Man unterscheidet zwei Arten von Verschlüsselungsalgorithmen:

- **Symmetrisch**: Zum Chiffrieren und Dechiffrieren (Chiffrieren = Verschlüsseln) einer Information wird derselbe kryptographische Schlüssel verwendet. Folglich muss der Absender und der Empfänger im Besitz des gleichen Schlüssels sein. Ohne diesen Schlüssel ist es unmöglich[2], die Originalinformation wieder zurückzubekommen. Der heute am häufigsten verwendete symmetrische Algorithmus ist **DES** (Digital Encryption Standard). Andere Algorithmen sind z. B. IDEA, RC2 und RC4.

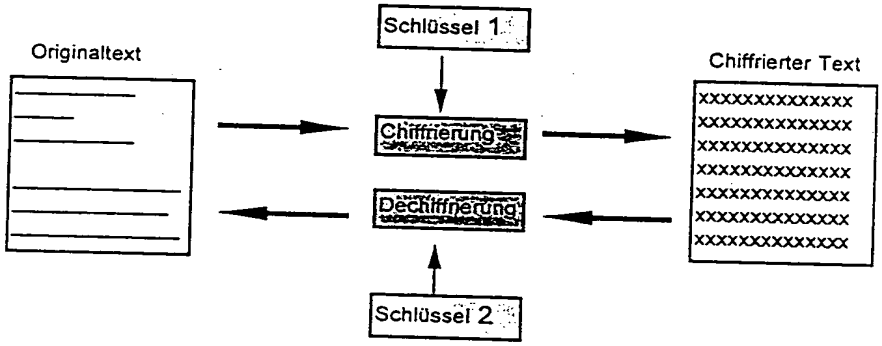


Symmetrischer Algorithmus

[1] Als Information wird hier eine Bitfolge bezeichnet. Sie kann verschiedenste Inhalte darstellen: Text, Bild, Video, Ton, Programmcode, usw.

[2] Unmöglich heisst hier, dass mit der heute mit Grossrechnern zur Verfügung stehenden Rechenleistung mehrere tausend Jahre benötigt werden, um einen Schlüssel zu knacken.

- **Asymmetrisch**: Zum Chiffrieren und Dechiffrieren werden zwei verschiedene, komplementäre Schlüssel verwendet (**Schlüsselpaar**); das heisst die Meldung wird mit dem Schlüssel 1 chiffriert und mit dem Schlüssel 2 dechiffriert. Diese Prozedur ist umkehrbar, d.h. es kann auch der Schlüssel 2 zum Chiffrieren und der Schlüssel 1 zum Dechiffrieren benützt werden. Es ist unmöglich[3], aufgrund des Schlüssels 1 den Schlüssel 2 zu rekonstruieren (oder umgekehrt). Ebenso ist es unmöglich, aufgrund der chiffrierten Information den Schlüssel zu berechnen. (Dies ist sogar dann gültig, wenn die Originalinformation bekannt ist.) Der heute mit Abstand am häufigsten verwendete asymmetrische Algorithmus ist **RSA** (benannt nach dessen Erfindern; Rivest, Shamir und Adleman). Eine Variante davon ist DSS (Digital Signature Standard).



Asymmetrischer Algorithmus

Mit Hilfe der asymmetrischen Chiffrierung kann eine sogenannte Digitale Signatur hergestellt werden. Wie das im Detail funktioniert, wird im folgenden erklärt.

4. Private und öffentliche Schlüssel

Mit Hilfe der asymmetrischen Verschlüsselungstechnik kann ein sogenanntes System von öffentlichen und privaten Schlüsseln realisiert werden. Dabei wird der eine Schlüssel des komplementären Schlüsselpaares als privat bezeichnet. Er ist im Besitz des Absenders und ist nur ihm bekannt. Er wird deshalb auch geheimer Schlüssel genannt (wobei dieser Begriff normalerweise für symmetrische Schlüssel verwendet wird). Der andere Schlüssel ist der öffentliche Schlüssel. Er ist allgemein zugänglich und wird an alle Teilnehmer verteilt. Wie oben erwähnt ist es nicht möglich, aufgrund des öffentlichen Schlüssels den privaten Schlüssel zu berechnen. Jeder Benützer erhält ein Schlüsselpaar bestehend aus dem privaten und dem öffentlichen Schlüssel. Dabei kann der Benützer sein eigenes Schlüsselpaar herstellen, oder er erhält es von einer vertrauenswürdigen Instanz.

Es ist von eminenter Wichtigkeit, dass der private Schlüssel auch wirklich geheim bleibt, d.h. dass keine andere Person ihn kennt, weil darauf die Sicherheit der Digitalen Signatur aufbaut. Darum ist es ratsam, den privaten Schlüssel nur in verschlüsselter Form auf dem PC abzulegen oder noch besser auf einer Chipkarte zu speichern, die mit einem PIN geschützt ist und auf der ausserdem der Chiffrieralgorythmus direkt implementiert ist. Auf diese Weise bleibt der private Schlüssel immer im Chip und verlässt diesen in keinem Moment. Die zu verschlüsselnden Daten werden in den Chip transferiert, dort werden sie verschlüsselt und

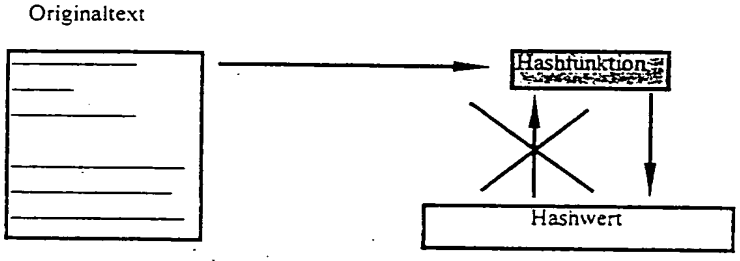
[3] Unmöglich heisst hier, dass mit der heute mit Grossrechnern zur Verfügung stehenden Rechenleistung mehrere tausend Jahre benötigt werden, um den komplementären Schlüssel zu finden.

anschliessend wieder zurückgesendet. Die Tatsache nämlich, dass der private Schlüssel in den Speicher des PC übergeführt wird, könnte nämlich ein Sicherheitsrisiko bedeuten, da es nie ausgeschlossen ist, dass im PC ein Virus steckt (unbemerkt), der systematisch den Speicher eines PC's abtastet und so den Schlüssel lesen könnte. Dieser wird dann z.B. an eine bestimmte IP-Adresse gesendet. Die Architektur des Chips ist so definiert, dass der private Schlüssel weder mit elektronischen noch mit optischen, mechanischen, chemischen oder elektromagnetischen Mitteln gelesen werden kann.

Im Gegensatz zum privaten Schlüssel ist der öffentliche Schlüssel allgemein bekannt und wird an alle Benützer verteilt. Der Einfachheit halber wird der öffentliche Schlüssel in der Regel mit jeder Meldung mitgeschickt. Wie wir weiter unten sehen werden, braucht es dabei eine vertrauenswürdige Instanz (Zertifizierungsinstanz) für die Echtheit der öffentlichen Schlüssel bürgt, da ein Krimineller sein eigenes Schlüsselpaar herstellen und sich als jemand anderen ausgeben kann. Diese Echtheitsgarantie geschieht in Form eines sogenannten Zertifikats, was im folgenden genauer beschrieben wird.

5. Die Hashfunktion

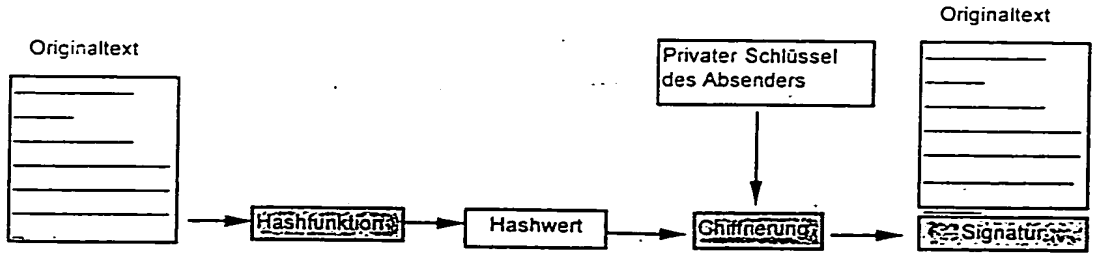
Die Hashfunktion ist ein **nicht-reziproker** Algorithmus, der aufgrund einer bestimmten Information beliebiger Länge einen **Hashwert (Kurzfassung/Komprimat)** fixer Länge herstellt. Er ist mit der Quersumme einer ganzen Zahl vergleichbar. Dabei ist die Länge der Meldung typischerweise um einiges grösser als der daraus berechnete Hashwert. So kann die Meldung z.B. mehrere Megabytes umfassen, wogegen der Hashwert nur 128 Bits lang ist. Es ist zu beachten, dass aufgrund des Hashwerts nicht auf die Originalinformation zurückgeschlossen werden kann (Nichtreziprokität), und dass es extrem schwierig ist, die Information so zu modifizieren, dass sie den gleichen Hashwert ergibt. Zweck einer solchen Funktion ist die Herstellung einer kurzen, für das jeweilige Dokument einzigartigen Codes. Dieser wird für die Herstellung der *Digitalen Signatur* benützt. Beispiele von Hashalgorithmen sind MD4 (Message Digest 4), MD5, RIPE-MD und SHA (Secure Hash Algorithm).



Hashfunktion

6. Die Digitale (Elektronische) Signatur

Jeder Benützer erhält einen privaten und einen öffentlichen Schlüssel. Um eine Meldung digital zu signieren, wird er **mit dem privaten Schlüssel des Absenders chiffriert**. Das Resultat ist die Digitale Signatur. Da aber die so entstandene Signatur die gleiche Grösse wie die Originalmeldung aufweist (unter Umständen mehrere Megabytes), wird zuerst der Hashwert der Meldung berechnet. Wie oben erwähnt hat der Hashwert eine fixe Länge und ist für eine bestimmte Meldung einzigartig. Statt der Originalmeldung wird nun deren Hashwert unterschrieben. Die so entstandene Digitale Signatur wird dem Originaldokument beigefügt. Das ganze wird dann an den Empfänger verschickt.

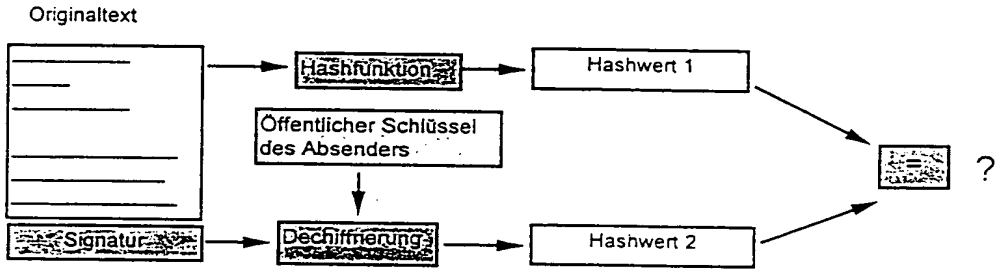


Digitale Signatur

Da nur der Absender des Dokumentes im Besitz seines privaten Schlüssels ist, kann nur er die Digitale Signatur herstellen. Hier liegt denn auch die Analogie zu einer handschriftlichen Unterschrift. Die digitale Signatur besitzt aber gewisse Eigenschaften, die bei der handschriftlichen Unterschrift nicht vorhanden sind. So kann z.B. bei einem handschriftlich unterschriebenen Vertrag nicht ausgeschlossen werden, dass keine Information ungeberkt hinzugefügt oder gelöscht wurde, was bei der digitalen Signatur nicht möglich ist. Die digitale Signatur bietet also sogar eine noch bessere Sicherheit als die traditionelle handschriftliche Unterschrift.

7. Überprüfung der Digitalen Signatur

Da der öffentliche Schlüssel an alle Benützer verteilt wird und somit allgemein bekannt ist, kann jeder Empfänger die Digitale Signatur überprüfen. Dazu dechiffriert er die Digitale Signatur **mit dem öffentlichem Schlüssel des Absenders**. Das Resultat ist der **Hashwert** der Originalmeldung. Parallel dazu berechnet der Empfänger den Hashwert des Originaldokuments, das ja ebenfalls (zusammen mit der Signatur) an ihn übermittelt wurde. Diesen resultierenden zweiten Hashwert **vergleicht** der Empfänger nun mit dem aus der Signatur dechiffrierten Hashwert. Stimmen die beiden Hashwerte miteinander überein, so ist die Digitale Signatur authentisch.



Überprüfung der digitalen Signatur

Wenn nun die Originalmeldung während der Übermittlung verändert wird (ein Bit genügt), so wird sich auch deren Hashwert verändern. Somit würde der Empfänger feststellen, dass der Hashwert den er aufgrund der Originalmelung berechnet hat, nicht mit dem aus der Signatur dechiffrierten Hashwert übereinstimmt, was bedeutet, dass die Signatur nicht korrekt ist.[4] Folglich hat der Empfänger bei einer erfolgreichen Überprüfung der digitalen Signatur die Garantie, dass die Meldung nicht verändert wurde (**Integrität**).

Da nur der Hersteller einer Signatur im Besitz seines privaten Schlüssels ist, kann nur er die Digitale Signatur herstellen. Dies bedeutet, dass der Empfänger, der die Digitale Signatur besitzt, nachweisen kann, dass nur der Absender die Signatur herstellen konnte (**Nichtabstreitbarkeit des Informationsursprungs**).

8. Zertifizierung des öffentlichen Schlüssels

Die Digitale Signatur ermöglicht also die Nichtabstreitbarkeit des Ursprungs und die Integritätsgarantie einer Meldung. Nun bleibt aber noch ein Sicherheitsproblem, nämlich die **Echtheitsgarantie des öffentlichen Schlüssels des Absenders**. Bis jetzt hat nämlich der Empfänger keine Garantie, dass der öffentliche Schlüssel tatsächlich derjenige des Absenders ist. Die Signatur kann zwar gültig sein, der damit verbundene öffentliche Schlüssel könnte aber theoretisch von einem Betrüger stammen.

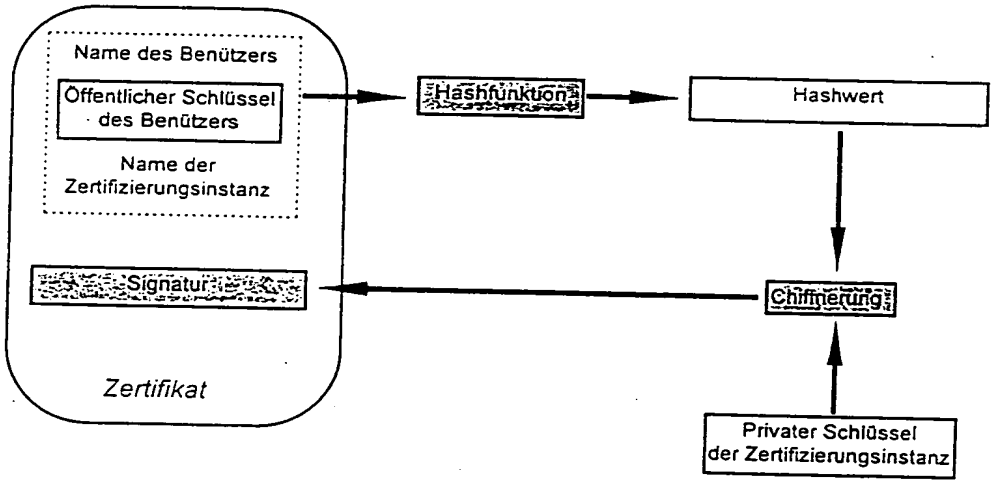
Nehmen wir an, ein Krimineller will jemanden zur Lieferung einer teuren Ware bewegen. Nichts hält ihn davon ab, selber einen öffentlichen und einen privaten Schlüssel zu generieren, die falsche Bestellung zu unterschreiben, und die Bestellung mit der Signatur zu versenden. Dann sendet er die mit seinem eigenen Schlüssel unterschriebene Bestellung mit dem öffentlichen Schlüssel an den Empfänger, und zwar **unter**

[4] Dies bedeutet, dass entweder die Information verändert wurde oder dass die digitale Signatur verändert wurde.

einem falschen Namen. Der Empfänger kann nicht feststellen, ob die Bestellung tatsächlich von der Person gesendet wurde, für die sie sich ausgibt. Die Signatur mag korrekt sein, aber der Empfänger hat keinen Anhaltspunkt dafür, dass der öffentliche Schlüssel, den er soeben erhalten hat, tatsächlich der richtigen Person gehört.

Der Empfänger einer Meldung braucht also die Gewissheit, dass der öffentliche Schlüssel des Absenders, in dessen Besitz er ist, tatsächlich dem richtigen Absender gehört. Diese Gewissheit kann er auf verschiedene Weise erlangen. Eine Möglichkeit ist, dass der Absender ihm den öffentlichen Schlüssel irgendwann einmal persönlich übergeben hat. Oder der Empfänger ruft den Absender an und vergleicht z.B. die ersten 10 Stellen des öffentlichen Schlüssels. Diese Methoden sind jedoch umständlich und bedingen, dass sich die Benützer entweder schon kennen oder sich vorher getroffen haben. Dies ist aber oft nicht der Fall. Nehmen wir an ein Schweizer will einem Schweden ein sicheres Email schicken, den er vorher noch nie gesehen hat und dessen Stimme er nicht kennt. Der Schwede könnte nun dem Schweizer seinen öffentlichen Schlüssel per Email schicken, jedoch hat der Schweizer keine Möglichkeit, die Echtheit dieses öffentlichen Schlüssels mit der dafür nötigen Gewissheit festzustellen.

Eine bessere wäre es, wenn es eine Instanz gäbe, welche die Zugehörigkeit eines öffentlichen Schlüssels zu einer gewissen Person garantiert. Diese Instanz wird **Zertifizierungsinstanz (Certification Authority / CA)** genannt und sie bürgt dafür, dass ein bestimmter öffentlicher Schlüssel einer bestimmten Person gehört.[5] Sie tut dies, indem sie ein sog. Zertifikat des öffentlichen Schlüssels herstellt. Es besteht im Wesentlichen aus dem öffentlichen Schlüssel und dem Namen des Besitzers. Das ganze wird dann von der Zertifizierungsinstanz signiert. Durch die Zertifizierung **bindet** die CA also einen öffentlichen Schlüssel an eine bestimmte Person (oder Maschine oder Prozess). Für alle Benützer wird so von der CA ein Zertifikat des öffentlichen Schlüssels ausgestellt. **Diese Zertifikate sind für alle Benützer zugänglich.**



Zertifizierung des öffentlichen Schlüssels durch die CA

Durch die Überprüfung der digitalen Signatur des Zertifikats des Absenders sowie der Signatur der Meldung selbst hat ein Empfänger den Beweis, dass die Meldung von demjenigen unterschrieben wurde, für den er sich ausgibt (**Authentifikation**).

Es ist zu beachten, dass die Schlüsselzertifikate nicht speziell geschützt werden müssen, da sie unfälschbar sind. Falls der Zertifikatsinhalt nämlich verändert wurde, merkt dies der Empfänger, da die Signatur nicht mehr korrekt ist. Und da niemand ausser der CA den privaten Schlüssel der CA hat, ist es niemandem möglich, die Signatur der CA zu fälschen.

Es gibt verschiedene Möglichkeiten, wie die Schlüsselzertifikate verbreitet werden. Eine Möglichkeit ist, die Zertifikate mit jeder Meldung mitzuschicken (mit dem Nachteil, dass dadurch die übertragene Datenmenge unter Umständen stark anwachsen kann). Um jedoch jemandem eine Vertrauliche, d.h. verschlüsselte

[5] Damit bürgt sie gleichzeitig dafür, dass der dazugehörige *private Schlüssel* der Person gehört.

Information zu übermitteln, **braucht der Absender das Zertifikat des Empfängers**. Falls er dieses nicht ha (z.B. bei der ersten Kontaktaufnahme) muss er es entweder direkt vom Empfänger verlangen, oder er holt es aus einem öffentlich zugänglichen Zertifikatsverzeichnis. Je nach Situation und Art der Benützer (innerhalb der Firma, weltweit, etc.) kann dieses Verzeichnis ein verteiltes Verzeichnis (X.500), ein Datenserver sein. Bei einer kleinen Anzahl von Benützern können die Zertifikate auch in einer einzigen, an alle verteilten Datei enthalten sein. Verschiedene Kombinationen sind ebenfalls denkbar. Besonders in einem multinationalen offenen System von potentiell vielen Benützern (tausende bis millionen) wird das Zertifikatsverzeichnis zu einer der wichtigsten Komponenten, da es die Schlüsselrolle bei der sicheren Kontaktaufnahme zweier Benützer einnimmt.

Mit Hilfe der oben beschriebenen Techniken können also zwei einander unbekannte Personen, Maschinen oder Prozesse gegenseitig Informationen austauschen, und dies auf eine sichere Art und Weise. Möglich wird dies durch die CA. Die grundlegende Bedingung ist dabei, dass die CA **das Vertrauen aller Benützer** geniesst. Theoretisch könnte die CA nämlich z.B. einen bestimmten öffentlichen Schlüssel unter einem falschen Namen zertifizieren (absichtlich oder durch Fahrlässigkeit). Dabei basiert das Vertrauen des Benützers in eine CA nicht auf rein technischen Aspekten, vielmehr hängt es von der Art ab, wie die CA ihre Dienste anbietet, wie seriös sie die Benützer identifiziert, wie sicher ihre physikalische Arbeitsungebung ist, welche Sicherheitsmassnahmen sie intern trifft, usw.

9. Verteilung des öffentlichen Schlüssels der Zertifizierungsinstanz

Nun bleibt noch ein letztes Problem. Wie im vorhergehenden Kapitel beschrieben, überprüft der Empfänger einer Meldung das Zertifikat des Absenders. Dazu benötigt er den öffentlichen Schlüssel der Zertifizierungsinstatz. Die CA könnte nun zwar ihren eigenen öffentlichen Schlüssel zertifizieren, dies macht aber wenig Sinn, da es ja jedem möglich ist, selber ein Schlüsselpaar zu generieren und selbst ein CA-Zertifikat (mit dem entsprechenden Namen der CA herzustellen. Für den öffentlichen Schlüssel der CA gibt es also **kein eigentliches Zertifikat**. Diese Tatsache erlaubt theoretisch einem Kriminellen, sich als Zertifizierungsinstanz auszugeben und so falsche Schlüsselpaare und Zertifikate herzustellen und zu verteilen. Darum muss der öffentliche Schlüssel der Zertifizierungsinstanz **auf einem sicheren Weg zum Benützer gelangen**. Der Benützer muss **überzeugt** sein, den richtigen Schlüssel der CA zu besitzen.

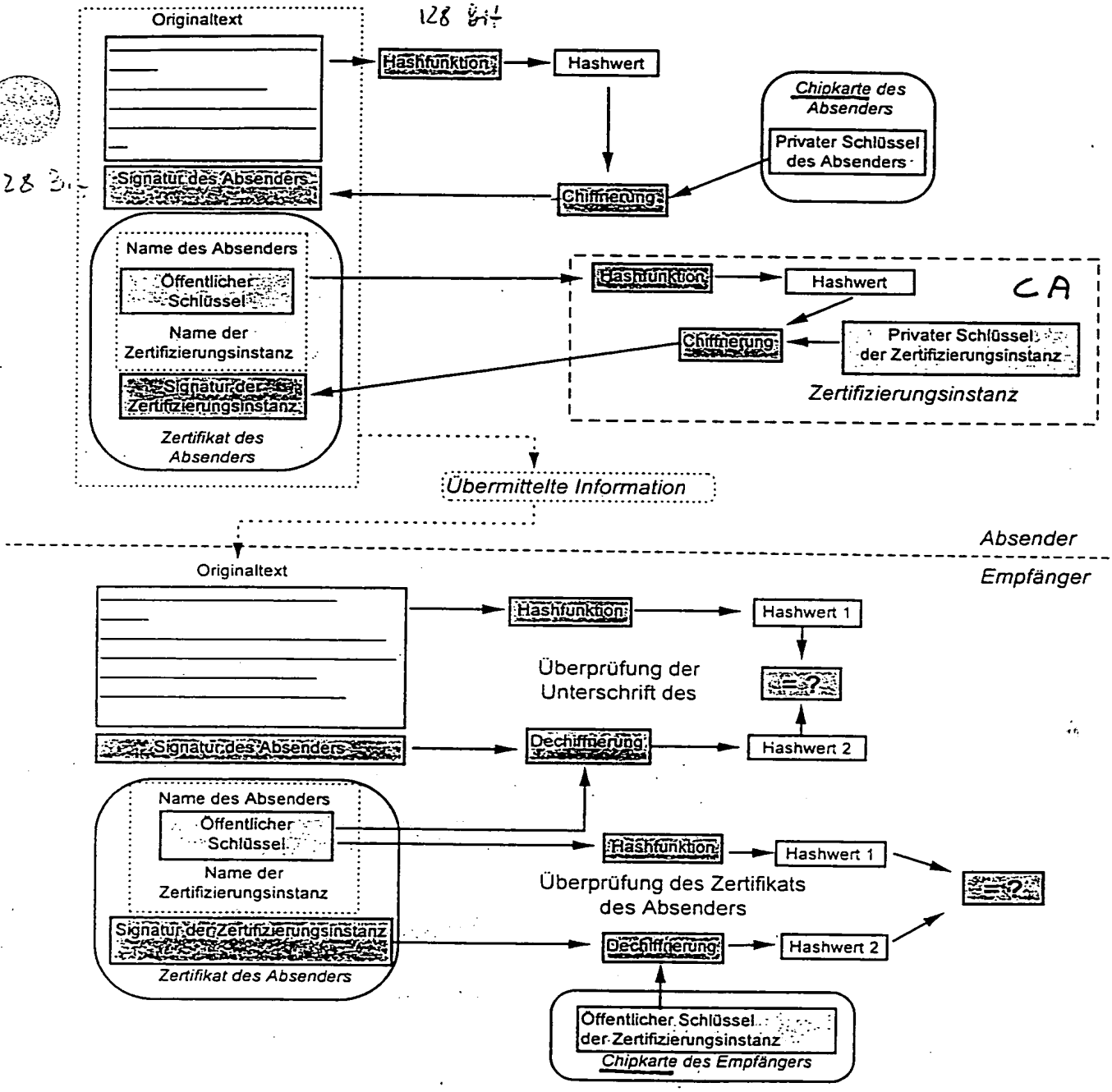
Eine Lösung, die sich sofort anbietet, ist, den öffentlichen Schlüssel der Zertifizierungsinstanz *in der Chipkarte des Benützers* zu speichern. Jener kann zwar (im Gegensatz zum privaten Schlüssel des Benützers) gelesen, aber nicht überschrieben oder gelöscht werden. Dies wird durch die spezielle Architektur des Chips erreicht.

Falls keine Chipkarten eingesetzt werden, muss der Schlüssel auf einem anderen sicheren Kanal zum Benützer gelangen (z.B. auf Diskette mit eingeschriebenem Brief).

Es ist ausserdem denkbar, dass der öffentliche Schlüssel der CA (oder Teile davon) so häufig publiziert, veröffentlicht und vervielfältigt wird (z.B. Telephonbücher, Telephonserver, Plakate, Verzeichnisdienste, usw.), dass ein Krimineller gar nicht die Möglichkeit hat, seinen falschen Schlüssel in gleichem Masse zu publizieren. In diesem Fall wird die Sicherheit durch die starke Publikation des öffentlichen Schlüssels der CA erreicht.

10. Übermittlung einer digital signierten Meldung ohne Chiffrierung: Zusammenfassung

- Der Absender unterschreibt die Meldung mit seinem privaten Schlüssel, um dessen Ursprung zu bestätigen.
- Die Originalmeldung wird zusammen mit der Signatur und dem Zertifikat des Absenders an den Empfänger gesendet.
- Der Empfänger überprüft die Digitale Signatur des Dokuments mit Hilfe des im Zertifikat des Absenders mitgeschickten öffentlichen Schlüssels des Absenders.
- Ausserdem versichert er sich der Echtheit des öffentlichen Schlüssels des Absenders, indem er die Digitale Signatur des Zertifikats überprüft. Dazu verwendet er den öffentlichen Schlüssel der Zertifizierungsinstanz.



Zusammenfassung: Digitale Signatur ohne Verschlüsselung

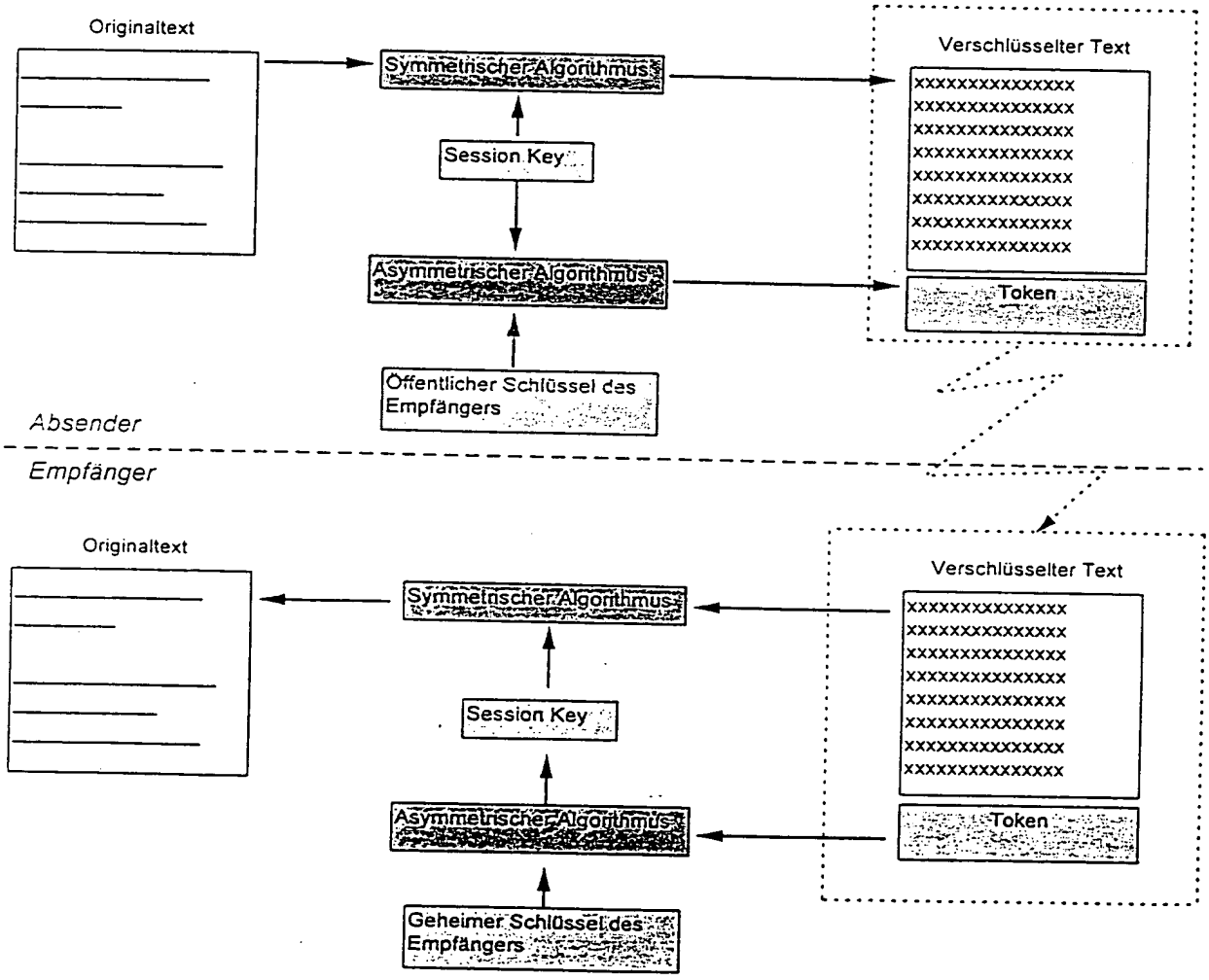
11. Chiffrierung der Meldung

Wenn die **Vertraulichkeit** einer Übermittlung, d.h. der Schutz vor der Einsichtnahme durch Unbefugte, gewährleistet sein soll, dann muss die Meldung verschlüsselt (chiffriert) werden. Dafür gibt es theoretisch zwei Möglichkeiten. Man könnte die Meldung mit dem öffentlichen Schlüssel des Empfängers verschlüsseln. Da nur der Empfänger im Besitz des dazugehörigen privaten Schlüssels ist, kann folglich nur er die Meldung

entschlüsseln. Nun ist es aber so, dass die asymmetrischen Chiffrieralgorithmen im Vergleich zu den symmetrischen **sehr langsam** sind. Wenn man sich vorstellt, dass die Meldung unter Umständen mehrere Megabytes umfassen kann, spielt dieser Zeitaufwand eine entscheidende Rolle. (Die Chiffrierung mehrerer Megabytes mit einem asymmetrischen Algorithmus benötigt je nach Rechenleistung Minuten bis Stunden.)

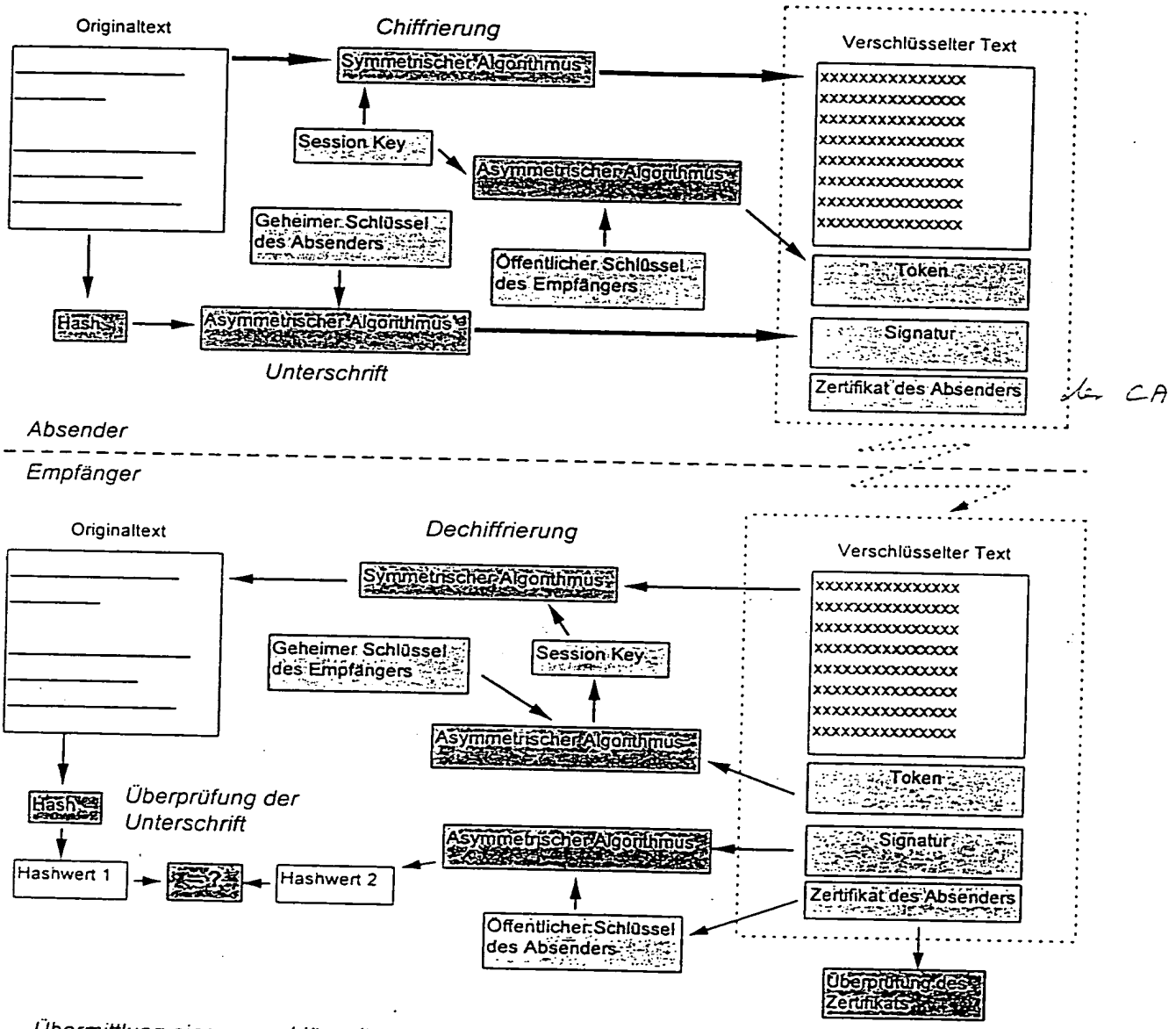
Darum weicht man in der Regel auf einen *symmetrischen Algorithmus* für die Chiffrierung der Meldung aus. Der Absender einer Meldung **generiert einen symmetrischen Schlüssel**, mit dessen Hilfe er die Meldung verschlüsselt. Diese symmetrische Verschlüsselung nimmt nur einen Bruchteil der Zeit in Anspruch, die bei der Verwendung eines asymmetrischen Algorithmus benötigt würde. (Sie beträgt typischerweise ein paar Sekunden). Dies bedeutet aber, dass der Empfänger *den selben symmetrischen Schlüssel* kennen muss. Er muss ihm also übermittelt werden, und zwar *verschlüsselt*, da sonst ein Betrüger den Schlüssel bei der Übertragung mitlesen und die Meldung entschlüsseln könnte. Darum wird der symmetrische Schlüssel, der sogenannte *Session Key*, mit dem **öffentlichen Schlüssel des Empfängers** verschlüsselt. Der so entstandene verschlüsselte Session Key wird auch *Token* genannt. Das Token enthält also den für die Chiffrierung der Meldung benützten symmetrischen Schlüssel, verschlüsselt mit dem öffentlichen (asymmetrischen) Schlüssel des Empfängers. Das Token wird zusammen mit der verschlüsselten Meldung, der Signatur und dem Zertifikat übermittelt.

Der Empfänger entschlüsselt das Token mit seinem privaten Schlüssel. So erhält er den für das Entschlüsseln der Meldung benötigten symmetrischen Schlüssel. Da nur er den privaten Schlüssel hat, kann nur er das Token entschlüsseln und somit die Meldung dechiffrieren (**Vertraulichkeit**).



Übermittlung einer verschlüsselten Meldung (ohne Unterschrift)

12. Übermittlung einer digital signierten Meldung mit Chiffrierung: Zusammenfassung



Übermittlung einer verschlüsselten und unterschriebenen Meldung

Absender:

- Der Absender unterschreibt die Meldung mit seinem privaten Schlüssel.
- Dann verschlüsselt er die Meldung mit einem von ihm generierten symmetrischen Schlüssel.
- Diesen symmetrischen Schlüssel verschlüsselt er dann mit dem öffentlichen Schlüssel des Empfängers. Daraus entsteht das Token.

- Die Originalmeldung wird dann zusammen mit der Signatur, dem Token und dem Zertifikat an den Empfänger gesendet.

Empfänger:

- Der Empfänger entschlüsselt zunächst das Token mit seinem privaten Schlüssel.
- Mit dem daraus gewonnenen symmetrischen Schlüssel entschlüsselt er die Meldung.
- Nun überprüft er die Digitale Signatur des Dokuments mit Hilfe des im Zertifikat des Absenders enthaltenen öffentlichen Schlüssels.
- Ausserdem versichert er sich der Echtheit des öffentlichen Schlüssels des Absenders, indem er die Digitale Signatur des Zertifikats durch die Zertifizierungsinstanz überprüft. Dazu verwendet er den öffentlichen Schlüssel der Zertifizierungsinstanz.

13. Revocation List / Ungültigerklärung von Zertifikaten

Nehmen wir an, einem Benützer wird seine Smart Card, welche seinen privaten Schlüssel enthält, mitsamt seinem PIN-Code gestohlen. Der Einbrecher kann nun diesen privaten Schlüssel einsetzen und sich für den Bestohlenen ausgeben, ohne dass dies der Empfänger merkt. Darum braucht es es einen Mechanismus, um allen Benützern mitzuteilen, dass das zum gestohlenen privaten Schlüssel gehörige Zertifikat nicht mehr gültig ist. Dies geschieht mittels einer sogenannte Liste von ungültigen Zertifikaten, einer *Certificate Revocation List (CRL)*. Sie wird von der CA digital signiert und veröffentlicht, d.h. sie wird allen Benützern zugänglich gemacht (entweder mittels eines Verzeichnisses oder mittels Zusendung der Liste an alle Benützer). Jeder Empfänger einer Meldung muss nun also zusätzlich zu der Überprüfung der Signatur und des Zertifikats des Absenders kontrollieren, ob letzteres sich nicht in der Revokation List befindet, d.h. ob es nicht ungültig ist. Falls dies aber der Fall ist, sollte der Empfänger der Signatur nicht trauen und sich bewusst sein, dass ein anderer als der angegebene Absender die Signatur geleistet haben könnte.

Damit die Revokation List nicht zu gross wird, wird statt des ganzen Zertifikats nur die Seriennummer sowie das Datum, an dem das Zertifikat für ungültig erklärt wurde, eingefügt. Die Liste besteht also aus Seriennummern und Ungültigkeitserklärungsdaten, welche am Schluss von der CA digital signiert wird. Vorhanden sind ebenfalls das Veröffentlichkeitsdatum der Liste und der Name der CA.

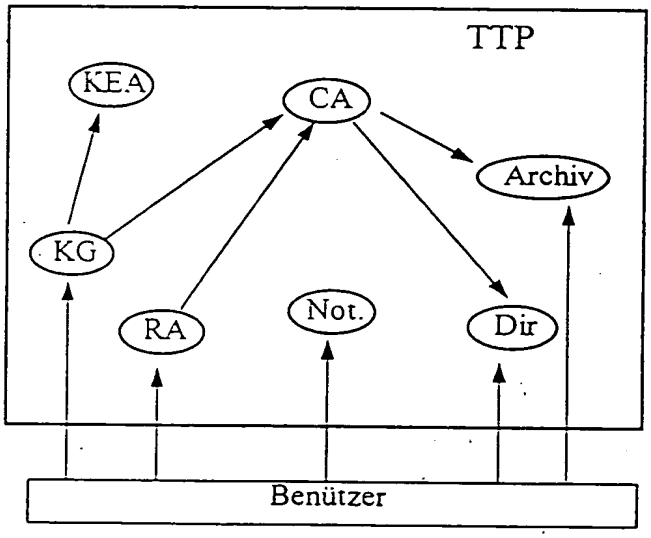
14. Das Trust Center und Trusted-Third-Party Dienste

Wie wir oben gesehen haben, braucht es in einem offenen und verteilten System von vielen Benützern, in dem zwei Benützer, die über kein gemeinsames Vertrauensverhältnis verfügen, sicher miteinander kommunizieren wollen, eine dritte Stelle, die diesen Benützern gewisse Sicherheitsdienste zur Verfügung stellt, da nämlich sonst für die Benützer der Aufwand zu gross wird selber die notwendigen Schlüssel auszutauschen und zu verwalten. Diese Stelle wird *Trust Center* oder *Trusted-Third-Party (TTP)* genannt und die Dienste, die sie anbietet, werden als *TTP-Dienste* bezeichnet. Die CA ist z.B. ein solcher Dienst. Die TTP übernimmt die Schlüsselverwaltungsaufgaben für die Benützer und geniesst darum deren Vertrauen. TTP-Dienste dienen zur also Sicherung von diversen Applikationen und Protokollen. Da die Sicherheitsmechanismen immer die gleichen sind, kann ein Kunde denselben TTP-Dienst für diverse Applikationen und Netzwerkprotokolle beanspruchen.

Die Bestandteile einer Trusted-Third-Party sind:

- **Registrierungsinstanz (RA)**: Sie identifiziert die Benützer, nimmt ihre Daten auf und leitet sie an die Zertifizierungsinstanz weiter. Die Identifikation der Benützer ist nötig, da ja die CA dafür garantiert, dass ein bestimmter öffentlicher Schlüssel einer bestimmten Person gehört. Dafür muss sich diese Person aber zuerst identifizieren.
- **Zertifizierungsinstanz (CA)**: Sie stellt die Schlüsselzertifikate und Revocation Lists her. Diese werden anschliessend zur Veröffentlichung in ein Verzeichnis abgelegt oder direkt den Benützer zugesandt.
- **Schlüsselgenerierungsdienst**: Er generiert die Schlüssel für die Benützer. Der private Schlüssel wird auf einem sicheren Kanal dem Benützer übergeben, der öffentliche Schlüssel wird an die CA gesendet zwecks Zertifizierung.
- **Schlüsselpersonalisierungsdienst:** Er legt die privaten Schlüssel in einem Modul (z.B. einer Chipkarte) ab, um sie vor unbefugtem Zugriff zu schützen.
- **Schlüsselhinterlegungsdienst (Key Escrow):** Er speichert eine Kopie der verwendeten Schlüssel. (Zwecks Rückerstattung im Falle eines Verlusts oder zwecks "Abhören" der Polizei aus Staatsschutz- oder Verbrechensbekämpfungsgründen).
- **Archivierungsdienst**: Er archiviert die Schlüsselzertifikate (zwecks langfristiger Garantie der Überprüfbarkeit von digitalen Signaturen)
- **Verzeichnisdienst**: Er stellt den Benützern Schlüsselzertifikate und Revocation Lists zur Verfügung.
- **Notariatsdienste** für
    1. Sende- und Empfangsbeweis
    2. Zeitstempel
    3. Beglaubigung der inhaltlichen Korrektheit (analog zu bestehenden Notariatsdiensten)

Der hier verwendete Begriff "Benützer" beschränkt sich nicht nur auf eine Person, sondern es kann damit auch eine Maschine ein Hardwaremodul oder sogar ein einzelner Prozess gemeint sein.



Abkürzungen:

CA	Certification Authority / Zertifizierungsinstanz
RA	Registration Authority / Registrierungsinstanz
KG	Key Generation / Schlüsselgenerierungsstelle
KEA	Key Escrow Agency / Schlüsselhinterlegungsstelle
Dir	Directory / Verzeichnisdienst
Not.	Notary / Notariatsdienste
Archiv	Archivierungsdienst für Zertifikate

Trusted-Third-Party ist also ein Oberbegriff, unter dem diverse TTP-Dienste gemeint sind. Eine TTP kann entweder alle oben beschriebenen Dienste anbieten oder nur eine Untermenge davon.

15. Schlussbemerkung: Transparenz der Sicherheitsabläufe für den Endbenützer

In den oben geschilderten Abläufen steht häufig geschrieben "Der Empfänger überprüft die Signatur" oder "Der Absender verschlüsselt die Meldung". Natürlich muss der Benützer all diese Funktionen im Normalfall nicht explizit selber ausführen, sondern das System macht das für ihn automatisch. Dabei sind diese Aktionen für den Benützer mehr oder weniger transparent, d.h. die Funktionen laufen zum Teil im Hintergrund ab. Der Benützer erfährt nur das Endresultat der verschiedenen Aktionen. Der Grad der Transparenz hängt

von der jeweiligen Implementierung sowie von der unterstützten Applikation ab. Wichtig ist allerdings, dass bei der Generierung der digitalen Signatur der Benützer explizit darauf hingewiesen wird, dass er nun im Begriff ist, eine solche zu tätigen.

Mobile - Cash

Variante 1: Client als MS beim POS

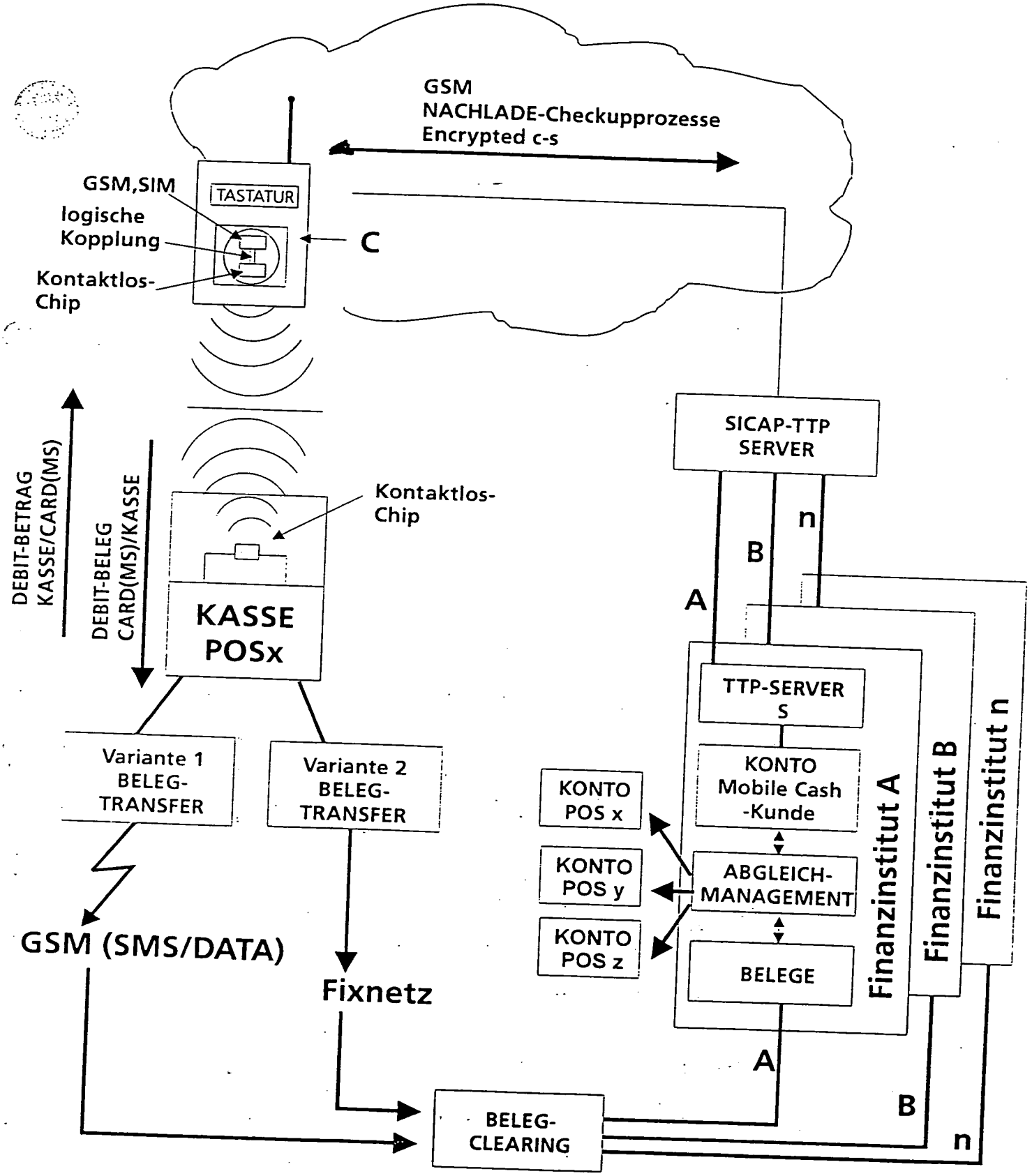


Fig. 1

Mobile - Cash

Variante 2: Client als MS interactiv mit PC

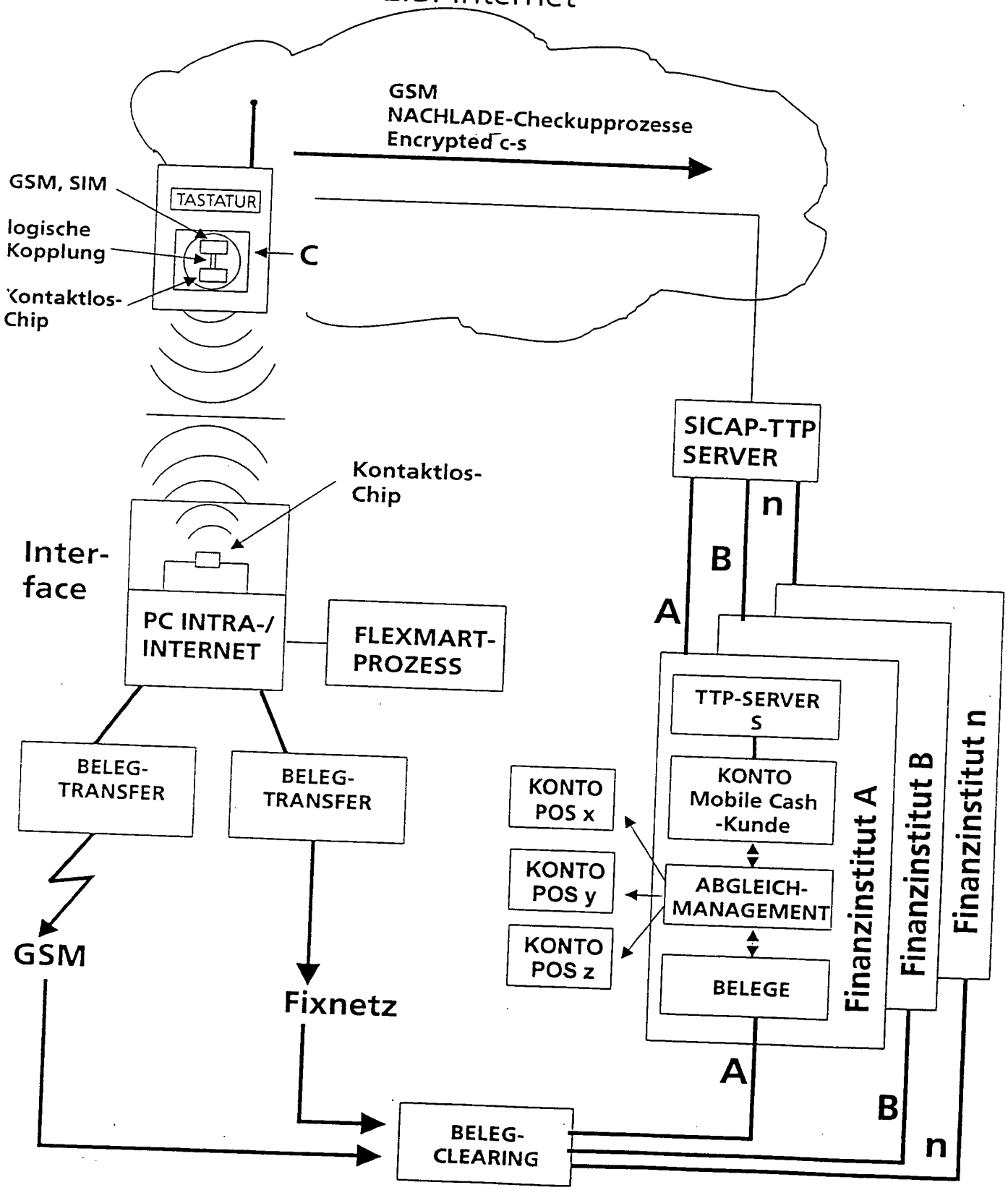
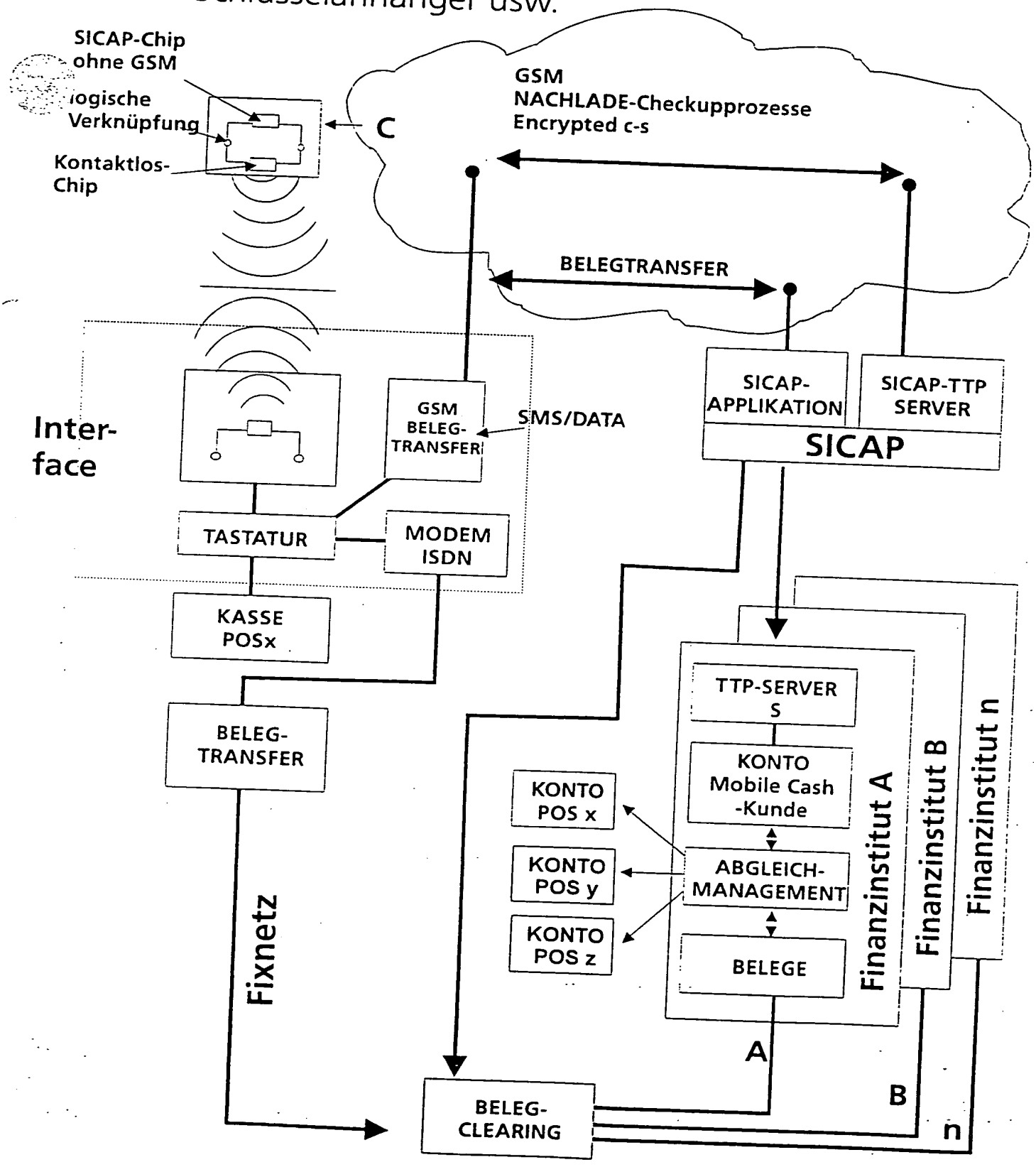


Fig. 2

Mobile - Cash

Variante 3: Client als Teilsystem auf Karte in Uhr, Schlüsselanhänger usw.

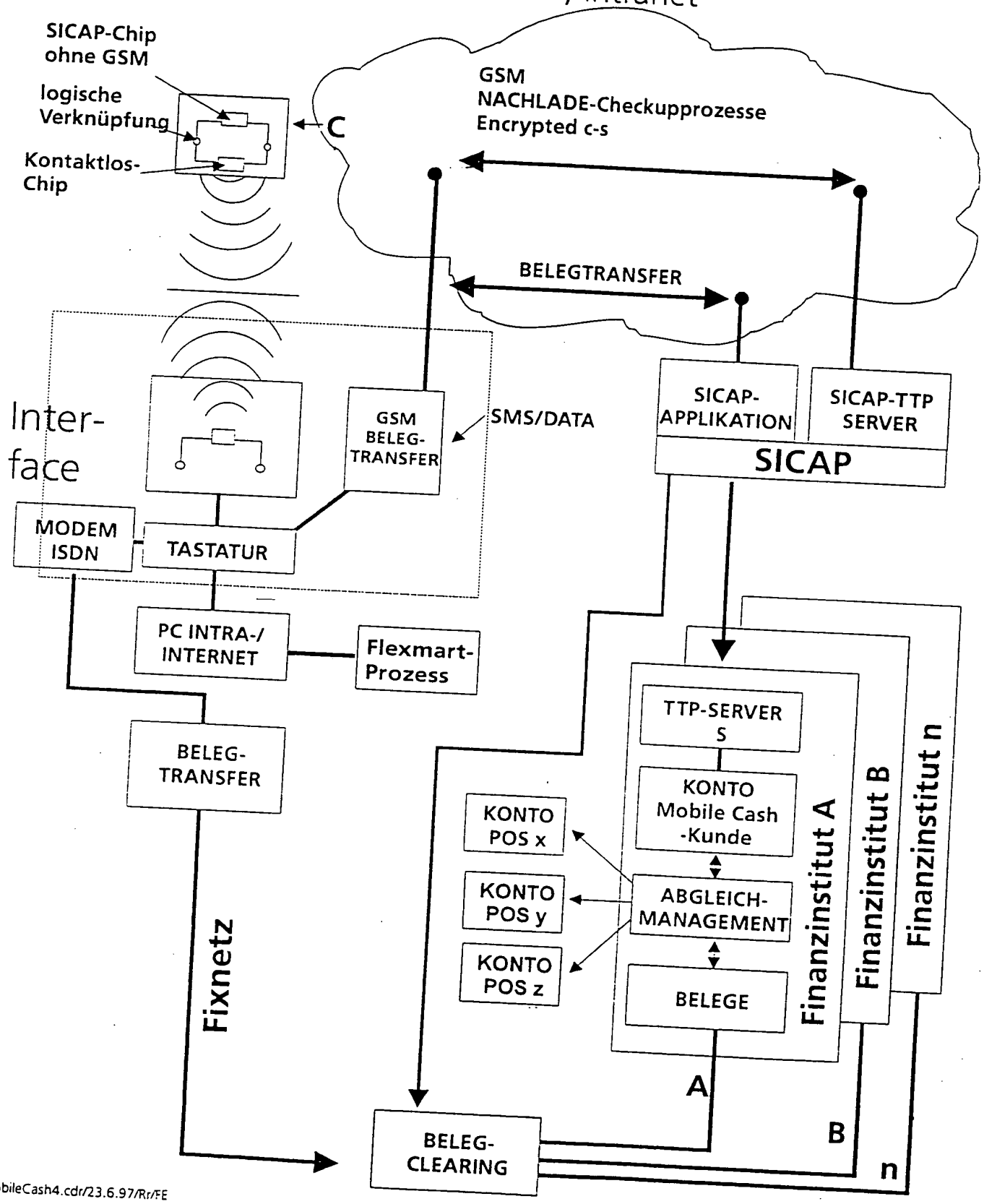


MobileCash3.cdr/23.6.97/Rr/FW

Fig. 3

Mobile - Cash

Variante 4: Client als Teilsystem auf Karte z.B. in Infrarotsteuerung mit PC/Inter-, Intranet



MobileCash4.cdr/23.6.97/Rr/FE

Fig. 4

Unveränderliches Exemplar
Exemplaire invariable
Esemplare immutabile

ZAHLUNGSTRANSAKTION

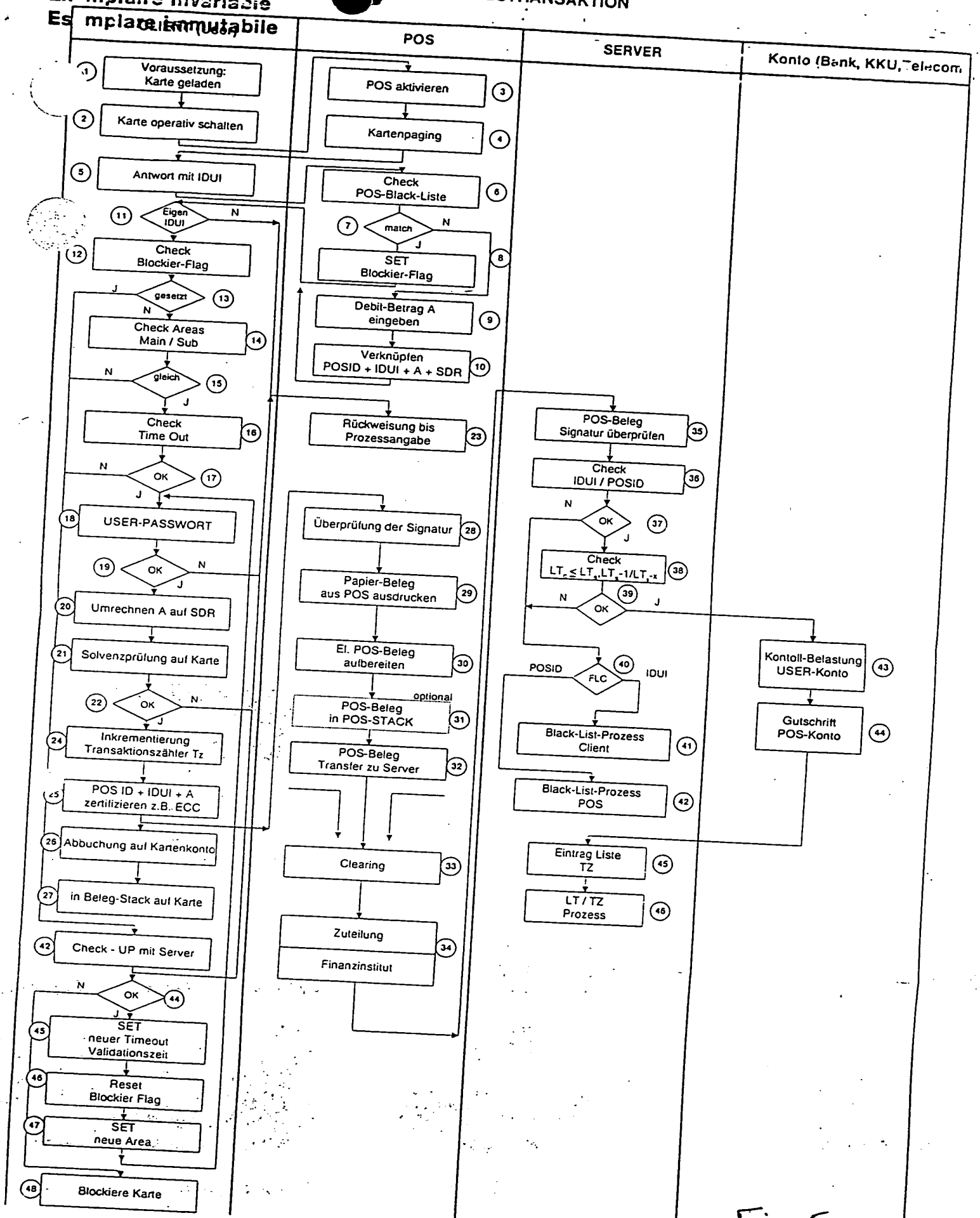


Fig. 5

PROZESS: NACHLADEN

Unveränderliches Exemplar
Exemplaire invariable
Esemplare immutabile

Checks wie "Area", "Time Out" sind in diesem Ablauf nicht nötig, weil der Check mit dem Server diese Prozesse enthält.

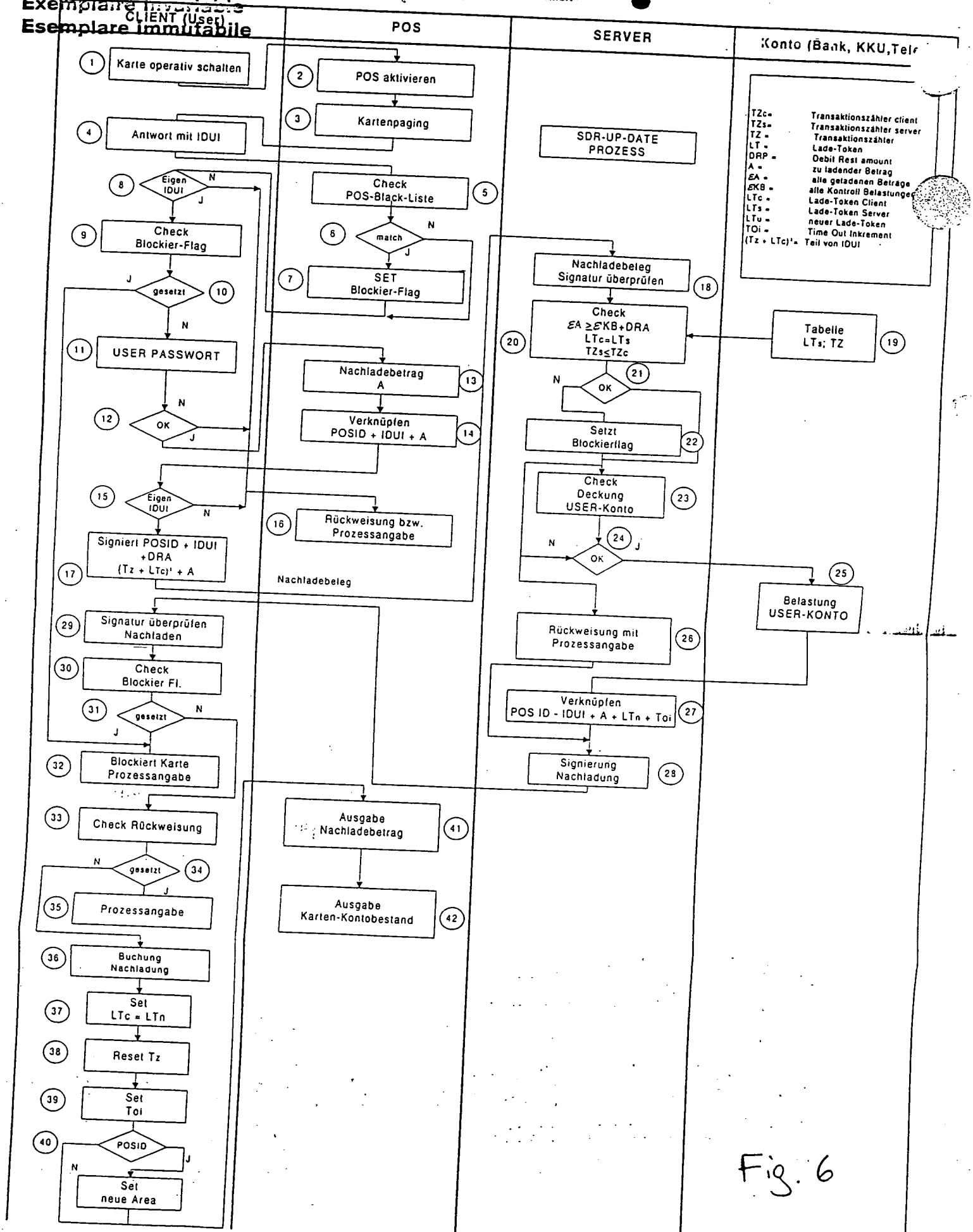


Fig. 6

Fall 1: Betragseingabe durch Kunde / Verkäufer mit EFTPOS

Kunde

Verkäufer

Clearing-Server

FTP

100.-

Ok

Kassa

*1234

EFTPOS-Terminal

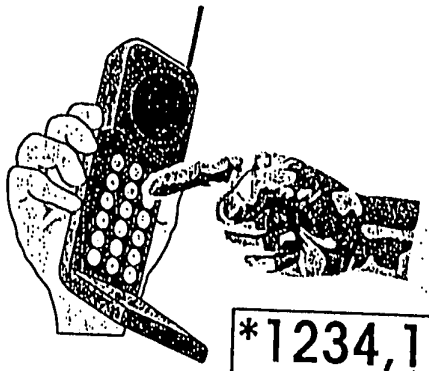
Kassa-Nr, 100.-

- BC
- Konto-Nr.
- Kassa-Nr.
- Betrag

Σ=0

Trans-aktion

1



*1234,100 PAY

(PIN)

SM

- 079...
- BC
- Konto-Nr.
- Kassa-Nr.
- Betrag

Timeout = 10 Sek

Fig. 7

Fall 2: Kunde nennt seine Natel-Nummer

Kunde

079...

Verkäufer

Kassa erfassen

- Betrag
- 079...
- Kassa-Nr.

SM

Server

Kundendaten
- 079...
- BC
- Konto-Nr.

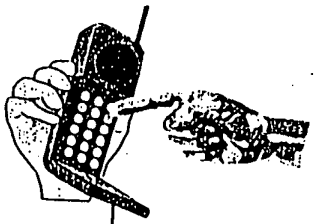
Verkäuferdaten
- Kassa
- BC
- Konto-Nr.

- Betrag

Freigabe

FTP

Trans-aktion



SM Betrag

SM Ok

Ok

F. 5.8

Fall 3: Betragseingabe durch Kunde / Verkäufer ohne ErTPOS

Kunde

Verkäufer

Kassa erfassen

Server

FTP

Trans-aktion

- BC
- Konto-Nr.
- Kassa-Nr. (Konto)
- Betrag

Σ=0

Kassa-Nr.

Betrag

SM

OK

- Kassa-Nr.
- Zeit
- Datum
- Betrag
- Gegenkonto (Benutzer)

Natel-Journal

SM

OK

Fig. 9

Unv ränderliches Exemplar
Ex mplaire invariabl
Esemplar immutabil